TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 18 mai 2000 (18.05.00)	
Demande internationale no PCT/FR99/02267	**Référence du dossier du déposant ou du mandataire** PF980065
Date du dépôt international (jour/mois/année) 23 septembre 1999 (23.09.99)	**Date de priorité** (jour/mois/année) 23 septembre 1998 (23.09.98)
Déposant CHEVREAU, Sylvain etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

11 avril 2000 (11.04.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

R. Forax

no de téléphone: (41-22) 338.83.38

M.H

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
PF980065		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 99/ 02267	23/09/1999	23/09/1998
Déposant		
THOMSON MULTIMEDIA et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 1

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
T/FR 99/02267

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 413 350 A (TOKYO SHIBAURA ELECTRIC CO) 20 février 1991 (1991-02-20) abrégé colonne 2, ligne 30 -colonne 3, ligne 25 colonne 5, ligne 23 -colonne 9, ligne 5 figures 1-4	1-5,10
A	US 4 937 679 A (RYAN JOHN O) 26 juin 1990 (1990-06-26) abrégé; figure 1 colonne 3, ligne 2 - ligne 60	1,10
A	EP 0 416 663 A (MATSUSHITA ELECTRIC IND CO LTD) 13 mars 1991 (1991-03-13) abrégé colonne 4, ligne 40 -colonne 5, ligne 13 revendications 1,3; figure 2	1,5-7,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 novembre 1999	12/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schiwy-Rausch, G

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
T/FR 99/02267

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 735 752 A (SONY CORP) 2 octobre 1996 (1996-10-02)	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 99/02267

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0413350 A	20-02-1991	JP 1861103 C	08-08-1994
		JP 3075827 A	29-03-1991
		JP 5070176 B	04-10-1993
		DE 69032305 D	18-06-1998
		DE 69032305 T	08-10-1998
		US 5295187 A	15-03-1994
US 4937679 A	26-06-1990	US 5130810 A	14-07-1992
		AT 122835 T	15-06-1995
		DE 68922658 D	22-06-1995
		DE 68922658 T	19-10-1995
		EP 0348218 A	27-12-1989
		ES 2072300 T	16-07-1995
		HK 1002419 A	21-08-1998
		JP 2064947 A	05-03-1990
		KR 9406160 B	08-07-1994
		PH 26068 A	29-01-1992
		AT 96933 T	15-11-1993
		DE 3788020 D	09-12-1993
		DE 3788020 T	03-03-1994
		EP 0256753 A	24-02-1988
		ES 2044937 T	16-01-1994
		HK 1008109 A	30-04-1999
		IE 62247 B	11-01-1995
		JP 2881432 B	12-04-1999
		JP 63107281 A	12-05-1988
		US 4907093 A	06-03-1990
		US 4819098 A	04-04-1989
		US 5194965 A	16-03-1993
EP 0416663 A	13-03-1991	JP 2629372 B	09-07-1997
		JP 3097167 A	23-04-1991
		JP 2584067 B	19-02-1997
		JP 3102676 A	30-04-1991
		DE 69032036 D	19-03-1998
		DE 69032036 T	20-08-1998
		KR 9408688 B	24-09-1994
		US 5159502 A	27-10-1992
EP 0735752 A	02-10-1996	JP 8275127 A	18-10-1996
		AU 709546 B	02-09-1999
		AU 4826396 A	10-10-1996
		BR 9601234 A	06-01-1998
		CA 2172009 A	01-10-1996
		CN 1135142 A	06-11-1996
		US 5778064 A	07-07-1998

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) **Classification internationale des brevets** [7] : **G11B 20/00, G06F 1/00**

A1

(11) **Numéro de publication internationale:** **WO 00/17871**

(43) **Date de publication internationale:** 30 mars 2000 (30.03.00)

(21) **Numéro de la demande internationale:** PCT/FR99/02267

(22) **Date de dépôt international:** 23 septembre 1999 (23.09.99)

(30) **Données relatives à la priorité:**
98/11860 23 septembre 1998 (23.09.98) FR

(71) **Déposant** *(pour tous les Etats désignés sauf US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F–92100 Boulogne (FR).

(72) **Inventeurs; et**
(75) **Inventeurs/Déposants** *(US seulement)*: CHEVREAU, Sylvain [FR/FR]; Thomson Multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne (FR). FURON, Teddy [FR/FR]; Thomson Multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne (FR).

(74) **Mandataire:** KOHRS, Martin; Thomson Multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne (FR).

(81) **Etats désignés:** AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) **Title:** COPY PROTECTION METHOD FOR DIGITAL DATA STORED ON A MEDIUM

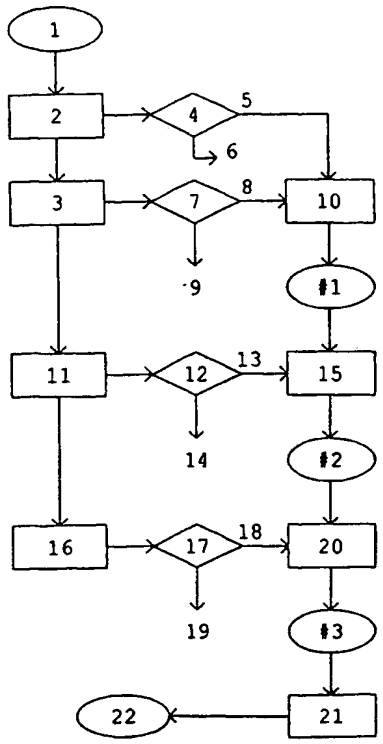
(54) **Titre:** PROTECTION CONTRE LA COPIE DE DONNEES NUMERIQUES STOCKEES SUR UN SUPPORT D'INFORMATIONS

(57) **Abstract**

The invention concerns a copy protection method for digital data stored on a medium (1) which consists, on the basis of a first digital data encryption identification (2) and a second digital data tattooing identification (3), in determining a first mark (#1) if the encryption and the tattooing have been identified (5, 8). A third identification of a type of storage medium (11) is followed by the determination (15) of a second mark (#2) if the first mark (#1) has been determined and if a type of storage medium has been identified (13). A fourth identification of cryptographic signature data (16) accompanying the digital data is followed by the determination (20) of a third mark (#3) if the second mark (#2) has been determined and if a cryptographic signature data has been identified (18). Permission for making a digital copy (22) of the digital data is then granted if the third mark (#3) has been determined.

(57) **Abrégé**

Une méthode de protection contre la copie de données numériques stockées sur un support d'informations (1) prévoit à partir d'une première identification d'un chiffrage (2) des données numériques et d'une seconde identification d'un tatouage (3) de données numériques de déterminer (10) une première marque (#1) si le chiffrage et le tatouage ont pu être identifiés (5, 8). Une troisième identification d'un type du support d'informations (11) est suivie de la détermination (15) d'une seconde marque (#2) si la première marque (#1) a pu être déterminée et si un type déterminé de support d'informations a pu être identifié (13). Une quatrième identification de données de signature cryptographique (16) accompagnant les données numériques est suivie de la détermination (20) d'une troisième marque (#3) si la seconde marque (#2) a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée (18). Une permission de copie numérique (22) des données numériques est délivrée si la troisième marque (#3) a pu être déterminée.



PROTECTION CONTRE LA COPIE DE DONNEES NUMERIQUES STOCKEES SUR UN SUPPORT D'INFORMATIONS

L'invention concerne une méthode et un dispositif permettant de protéger contre la copie de données numériques stockées sur un support d'informations.

Une possibilité inhérente aux données numériques est qu'elles peuvent être copiées sans perte notable de qualité puisque la copie consiste à transmettre de la source à l'enregistreur une série de « 1 » et de « 0 ». Le plus grand nombre d'erreurs survenant éventuellement lors de la copie peuvent être palliées en utilisant des méthodes de correction d'erreur. Ainsi lorsqu'un support d'informations contient des données numériques, il est en principe relativement simple d'enregistrer à l'identique sur un support enregistrable le contenu du support d'informations.

De nombreux types et sortes de supports d'informations sont utilisé pour stocker de l'information de toute nature sous forme numérique. Par exemple une bande magnétique, un disque optique enregistrable ou non (CD, CD-R, CD-RW, DVD, DVD-R, disque Magneto-optique etc., respectivements de l'anglais Compact Disc, CD-Recordable, CD-Read Write, Digital Versatile Disc, DVD-Recordable) peut stocker de l'information audio et / ou vidéo sous forme numérique.

Afin de mieux préserver par exemple les intérêts des auteurs de l'information stockée ou ceux de producteurs de support d'informations préenregistré, il est désirable de limiter les possibilités de copier librement et simplement les données numériques. Divers mécanismes et possibilités existent actuellement pour protéger des données numérique contre une copie illégitime.

De façon connue les données numériques peuvent être chiffrées lorsqu'elles sont stockées sur le support d'informations. Le chiffrage permet de limiter l'utilisation des données numériques au détenteur d'une clé publique ou privée de déchiffrage. Le chiffrage est par exemple utilisé dans la protection de données sur les DVD, disques optiques utilisés pour stocker des données vidéo sous forme numérique. Ainsi un lecteur de DVD nécessite une clé appropriée pour déchiffrer les données lues sur le DVD.

Une façon de protéger des données numériques contre la copie consiste à les doter d'un tatouage, c'est-à-dire de données auxiliaires attachées aux données numériques. Le tatouage doit être non-modifiable et non effaçable. La lecture des données se fait à l'aide d'une clé publique qui identifie le tatouage.

L'information de gestion des générations ne permet pas d'éviter en soi les copies par voie analogique.

Un objet de l'invention consiste à trouver une solution de protection contre la copie numérique dans laquelle aucune information relative à la génération de copie est disponible en clair lors de la copie.

Un autre objet de l'invention consiste à trouver une solution dans laquelle aucune modification de données relatives à la protection contre la copie soit entreprise à l'enregistrement éventuelle d'une copie.

Une solution que propose l'invention prévoit une méthode de protection contre la copie de données numériques stockées sur un support d'informations, comprenant

une première identification d'un chiffrage des données numériques,

une seconde identification d'un tatouage de données numériques,

une première détermination d'une première marque si le chiffrage et le tatouage ont pu être identifiés,

une troisième identification d'un type du support d'informations,

une seconde détermination d'une seconde marque si la première marque a pu être déterminée et si un type déterminé de support d'informations a pu être identifié,

une quatrième identification de données de signature cryptographique accompagnant les données numériques,

une troisième détermination d'une troisième marque si la seconde marque a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée,

une première délivrance d'une permission de copie numérique des données numériques si la troisième marque a pu être déterminée.

Une première réalisation avantageuse de l'invention prévoit une seconde délivrance d'une interdiction de lecture des données numériques si la première identification est négative et si le tatouage a pu être identifié, ou si le chiffrage a pu être identifié et la seconde identification est négative.

Une deuxième réalisation avantageuse de l'invention prévoit une troisième délivrance d'une permission de copie numérique des données numériques si la première et la seconde identifications sont négatives.

Une troisième réalisation avantageuse de l'invention prévoit une quatrième délivrance d'une interdiction de copie numérique des données numériques si la première marque a pu être déterminée et si la troisième identification révèle un type différent du type déterminé de support d'informations.

une partie de contrôle de l'enregistrement qui permet de gérer un flux de données numériques vers la sortie numérique lorsqu'elle reçoit notamment un signal de permission de copie,

un système de protection pour la lecture recevant des signaux du système de déchiffrage et générant un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées, ou lorsque les données numériques sont chiffrées mais non tatouées,

une partie de contrôle de la lecture qui permet d'interrompre la lecture des données ou leur sortie vers la sortie analogique lorsqu'elle reçoit notamment un signal d'interdiction de lecture.

Dans la suite, des exemples de réalisation sont présentés qui permettront d'illustrer et de mieux comprendre l'invention, en faisant référence aux figures 1 à 8, brièvement décrites ci-dessous :

Fig. 1 contient un organigramme illustrant un mode de réalisation de l'invention,

Fig. 2 à 5 contiennent des organigrammes illustrant des aspects de l'invention,

Fig. 6 contient un organigramme illustrant une conversion numérique-analogique selon l'invention,

Fig. 7 contient un organigramme illustrant des aspects de l'invention relatifs au chiffrage,

fig. 8 contient un schéma illustrant un dispositif selon l'invention.

La Fig. 1 contient un organigramme dans lequel des données numériques stockées sur un support d'informations 1 sont soumises à une première identification d'un chiffrage 2 afin de vérifier si les données numériques sont stockées sous forme chiffrée, puis à une seconde identification d'un tatouage 3 pour voir si les données sont pourvues d'un tatouage numérique. Une première bifurcation 4 permet de distinguer les cas où un chiffrage est identifié 5 ou non 6. Une seconde bifurcation 7 permet de distinguer les cas où un tatouage est identifié 8 ou non 9. Si les cas 5 et 8 sont vérifiés une première détermination 10 génère une première marque #1.

Une troisième identification 11 d'un type du support d'informations 1 sert à voir si le support d'informations est par exemple du type non-enregistrable ou enregistrable. Une information sur le type peut être contenue dans les données numériques en soi où résulter de mesures physiques de paramètres du support d'informations 1 lors par exemple d'une initialisation dans un lecteur du support d'informations 1. Une troisième bifurcation 12 permet de distinguer les cas où le

cas 8, c'est-à dire qu'un tatouage est présent. Alors une seconde délivrance 23 génère une interdiction de lecture des données numériques 24. En pratique cela pourrait par exemple conduire à une interruption de la lecture des données. Un autre cas de figure prévoit que la première bifurcation 4 livre le cas 5, c'est-à dire qu'un chiffrage est identifié, et que la seconde bifurcation 7 livre le cas 9, c'est -à dire que la seconde identification d'un tatouage est négative. Dans cet autre cas la seconde délivrance génère l'interdiction de lecture 24.

La méthode décrite permet de copier librement des données numériques qui ne sont pas protégées, par exemple des données dépourvues de chiffrage et de tatouage. La Fig. 3 contient un organigramme dans lequel la première et la seconde bifurcation 4 et 7 livrent chacune un cas d'identification négative respectivement les cas 6 pour le chiffrage et 9 pour le tatouage. Une troisième délivrance 25 génère alors directement la permission de copie numérique 22.

Dans le dernier cas il importe peut que les données soient sur un support d'informations enregistrable ou non. L'absence de chiffrage et de tatouage indique un niveau de protection des données minimum.

Dans certains cas de figure les données doivent pouvoir être lues et exploitées mais non copiées. C'est le cas notamment lorsque l'on achète un support d'informations contenant des données numériques dont l'auteur ou le producteur veut éviter la copie. C'est le cas également lorsqu'un support d'informations enregistrable contenant des données copiées légalement est lu. Un tel cas est illustré à l'aide d'un organigramme dans la Fig. 4 où une quatrième délivrance 26 vérifie que la première marque #1 a été délivrée et que le cas 14 d'identification d'un type de support d'informations différent du type déterminé ait eu lieu avant de générer une interdiction de copie 27. En pratique le lecteur devrait mettre en oeuvre un dispositif empêchant une copie des données numériques, par exemple en inhibant une sortie numérique du lecteur.

Un autre tel cas est illustré à l'aide d'un organigramme dans la Fig. 5. Si la deuxième marque #2 est identifiée et le cas 19 signalise une quatrième identification négative, c'est à dire qu'aucune signature cryptographique permettant une copie des données est présente, alors une cinquième délivrance 28 génère l'interdiction de copie 27.

Il est entendu que le fait qu'aucune signature cryptographique permettant une copie des données soit identifié n'exclut pas la présence d'une signature cryptographique particulière interdisant la copie.

signature cryptographique déchiffrée 38. Cette dernière est chiffrée lors d'un premier chiffrage 39 à l'aide d'une clé publique 40 contenue dans le lecteur avant d'être acheminée sous forme de signature cryptographique chiffrée 41 vers une sortie numérique (non illustrée) ensemble avec les données numériques chiffrées 411 lors d'un second chiffrage 399 à l'aide de la clé privée 400. Ainsi aucune manipulation des données et du tatouage n'est possible.

Un dispositif de lecture de données numériques 42 illustré à la Fig. 8 comprend une sortie numérique 43 qui permet de livrer des signaux représentatifs des données numériques lors d'un lecture des données numérique d'un support d'informations. Cette sortie 43 peut par exemple être réalisée à l'aide d'un bus numérique au standard IEEE1394. Une sortie analogique 44 permet de livrer des signaux analogiques représentatifs des mêmes données numériques. Un système de déchiffrage 45 permet de déchiffrer des données numériques si celles-ci sont chiffrées, mais aussi d'identifier un éventuel tatouage et des données de signature cryptographique. Le système de déchiffrage permet de mettre en oeuvre par exemple les identifications 2, 3, 11 et 16 de la méthode illustrée à la Fig. 1.

Un système de protection pour la copie des données numériques 46 utilise des signaux émis par le système de déchiffrage 45 et les évalue en implémentant les déterminations 10, 15 et 20 de la méthode illustrée à la Fig. 1, et délivre après avoir déterminé les marques #1, #2 et #3 un signal de permission de copie.

Une partie de contrôle de l'enregistrement 47 permet de gérer un flux de données numériques vers la sortie numérique. Cette partie peut notamment activer le flux lorsqu'elle obtient du système de protection 46 le signal de permission de copie.

Le système de protection pour la copie des données numériques 46 peut également jouer le rôle d'un système de protection pour la lecture. Ce dernier système génère à l'aide des signaux reçus du système de déchiffrage 45 un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées ou encore lorsque les données numériques sont chiffrées mais non tatouées.

Une partie de contrôle de la lecture 48 permet d'interrompre la lecture des données numériques lorsqu'elle reçoit le signal d'interdiction du système de protection pour la lecture.

32. détection
33. altération
34. signaux analogiques altérés
35. suppression de sortie des données numériques
36. déchiffrage des données numériques
37. données numériques déchiffrées
38. données de signature cryptographique déchiffrées
39. premier chiffrage
399. second chiffrage
40. clé publique
400. clé privée
41. signature cryptographique chiffrée
411. données numériques chiffrées
42. dispositif de lecture de données numériques
43. sortie numérique
44. sortie analogique
45. système de déchiffrage
46. système de protection pour la copie des données numériques
47. partie de contrôle de l'enregistrement
48. partie de contrôle de la lecture.

une quatrième délivrance (26) d'une interdiction de copie (27) numérique des données numériques si la première marque (#1) a pu être déterminée et si la troisième identification révèle un type différent (14) du type déterminé de support d'informations.

5. Une méthode de protection selon l'une quelconque des revendications 1 à 4, caractérisée en ce qu'elle comprend

une cinquième délivrance (28) d'une interdiction de copie (27) numérique des données numériques si la deuxième marque (#2) a pu être déterminée et si la quatrième identification est négative (19).

6. Une méthode de protection selon l'une quelconque des revendications 1, 4 ou 5, caractérisée en ce qu'elle comprend

une conversion (30) des données numériques (29) en signaux analogiques (31),

une altération (33) des signaux analogiques si la première (21), la quatrième (26) ou la cinquième délivrance (28) a été réalisée.

7. Une méthode de protection selon l'une quelconque des revendications 4 ou 5, caractérisée en ce que l'interdiction de copie numérique (27) comprend une suppression (35) de sortie des données numériques.

8. Une méthode de protection selon la revendication 1, caractérisée en ce qu'elle comprend

un déchiffrage des données numériques (36) si un chiffrage a pu être identifié afin d'obtenir des données numériques déchiffrées (37) et des données de signature cryptographique déchiffrées (38),

un premier chiffrage (39) des données de signature cryptographique à l'aide d'une clé publique (40).

9. Une méthode de protection selon la revendication 8, caractérisé en ce qu'elle comprend

un second chiffrage (399) des données numériques déchiffrées à l'aide d'une clé privée (400).

10. Un dispositif de lecture de données numériques stockées sur un support d'informations comprenant au moins,

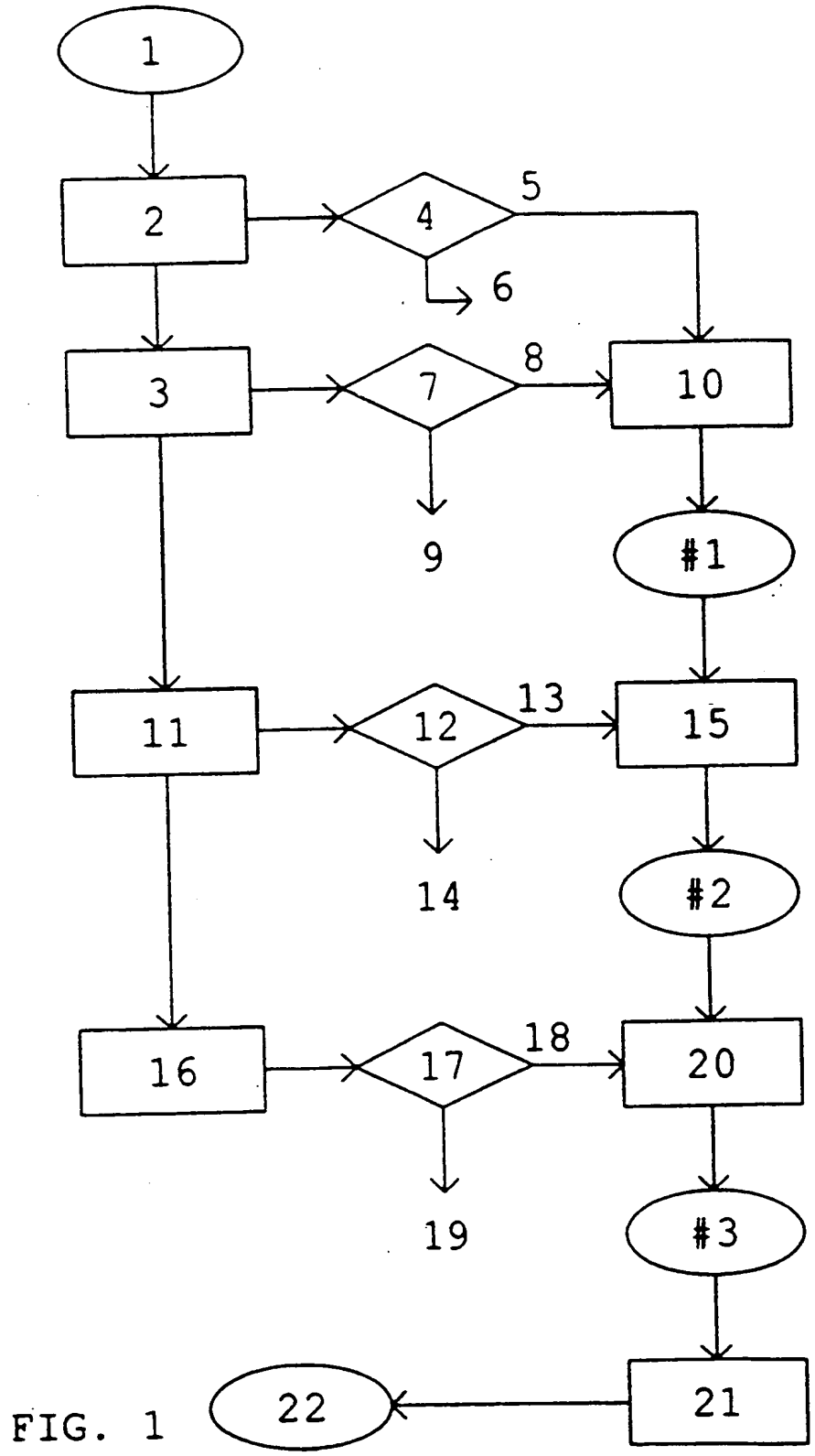


FIG. 1

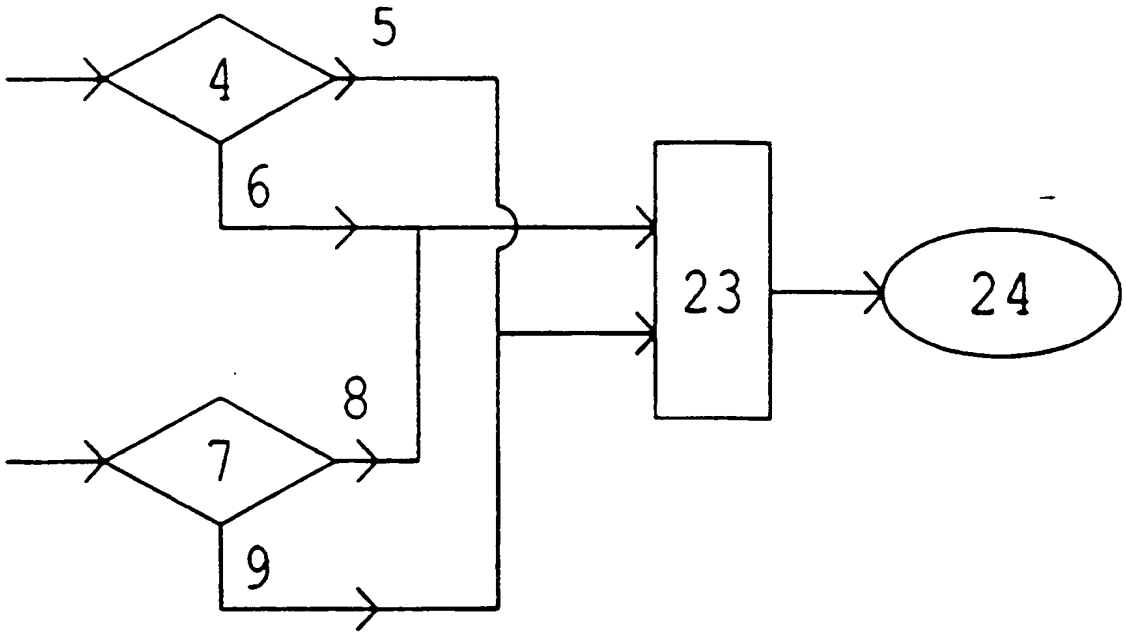


FIG. 2

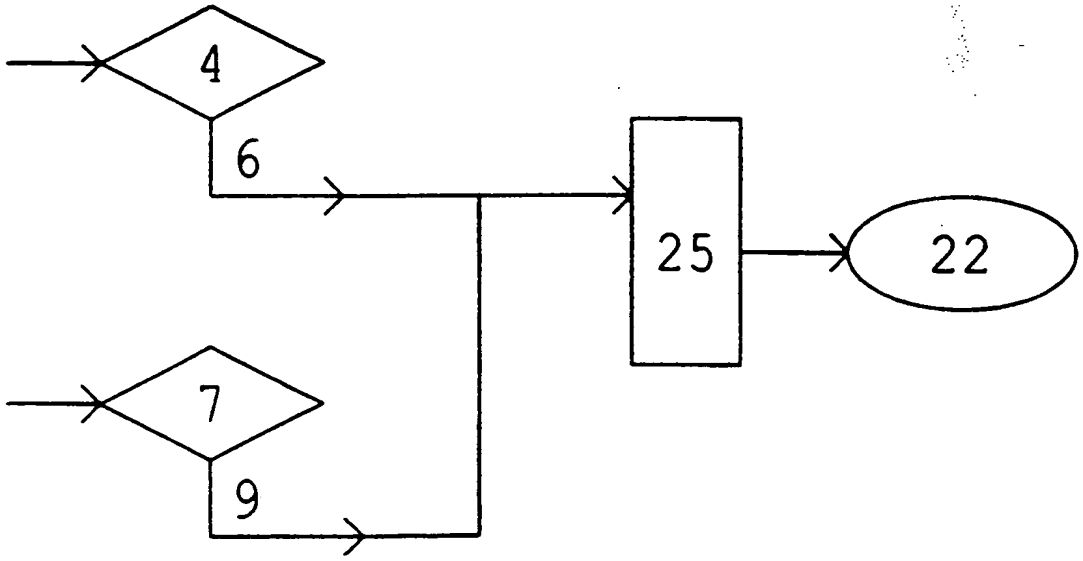


FIG. 3

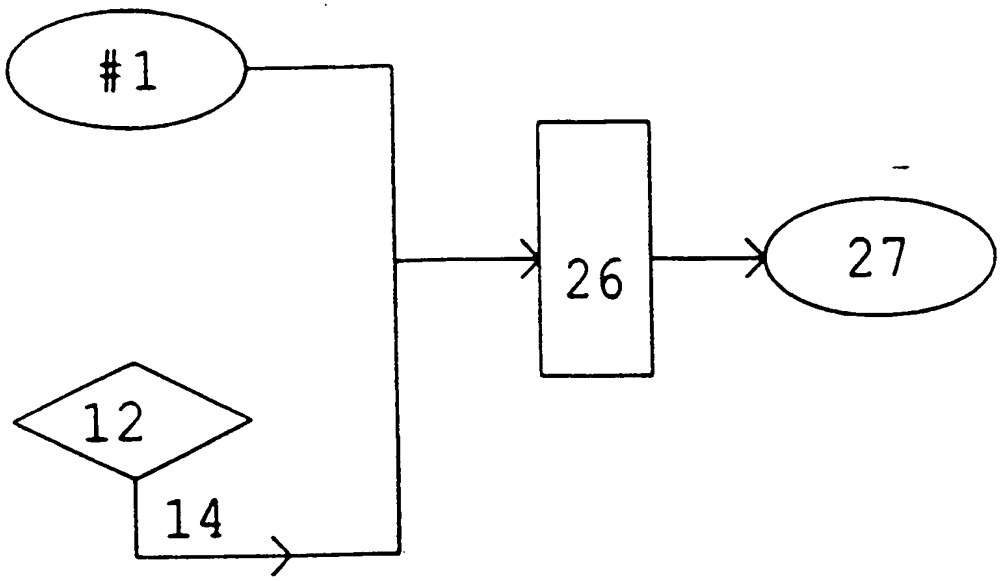


FIG. 4

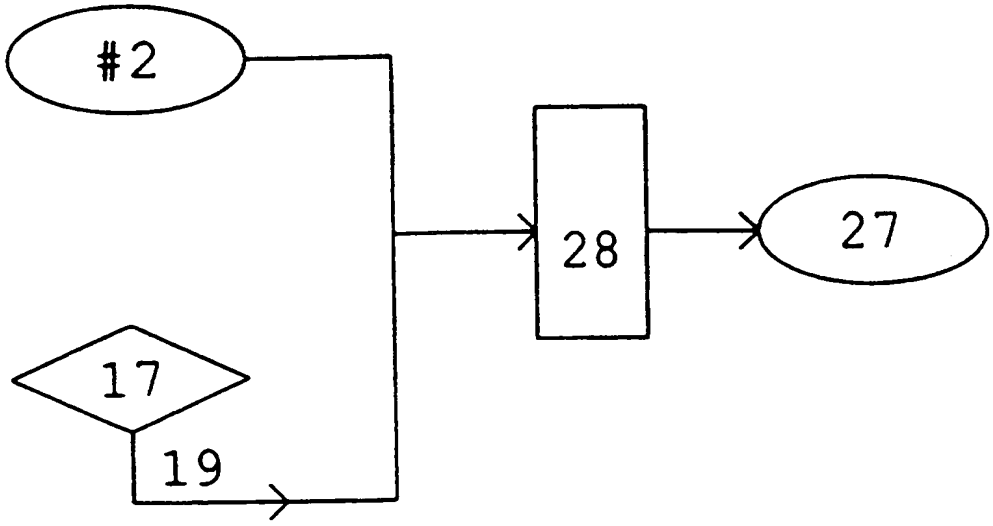


FIG. 5

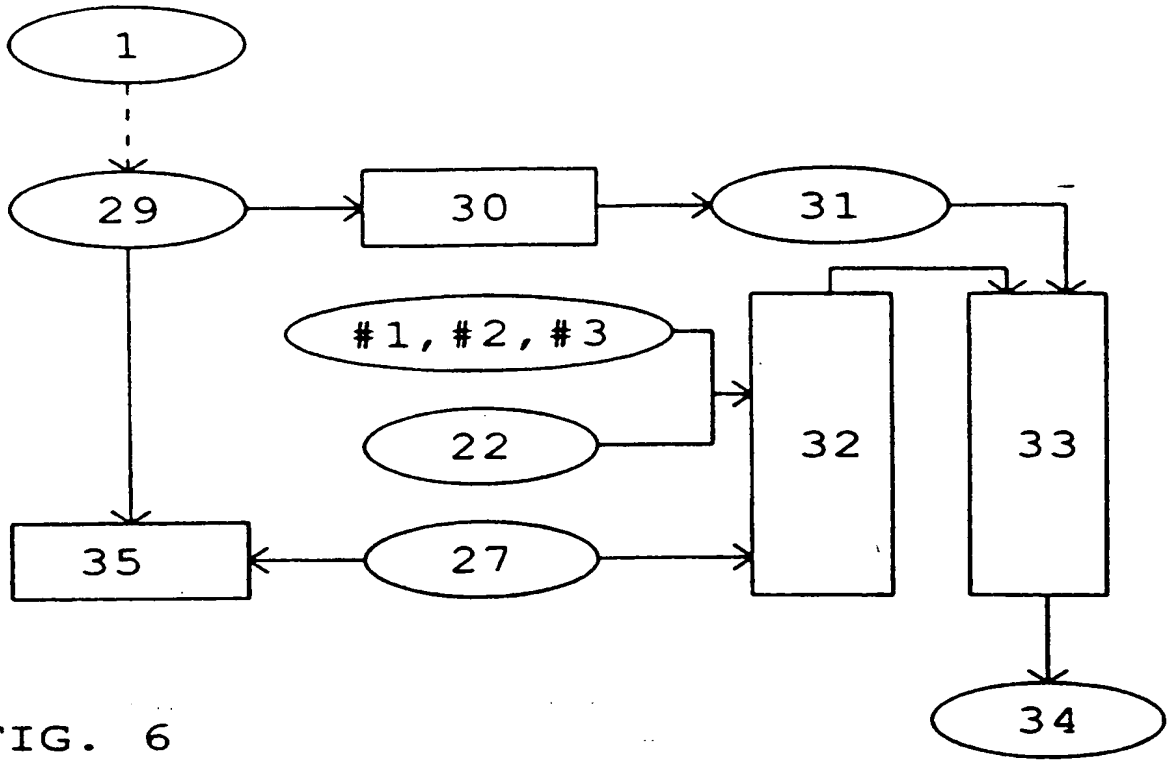


FIG. 6

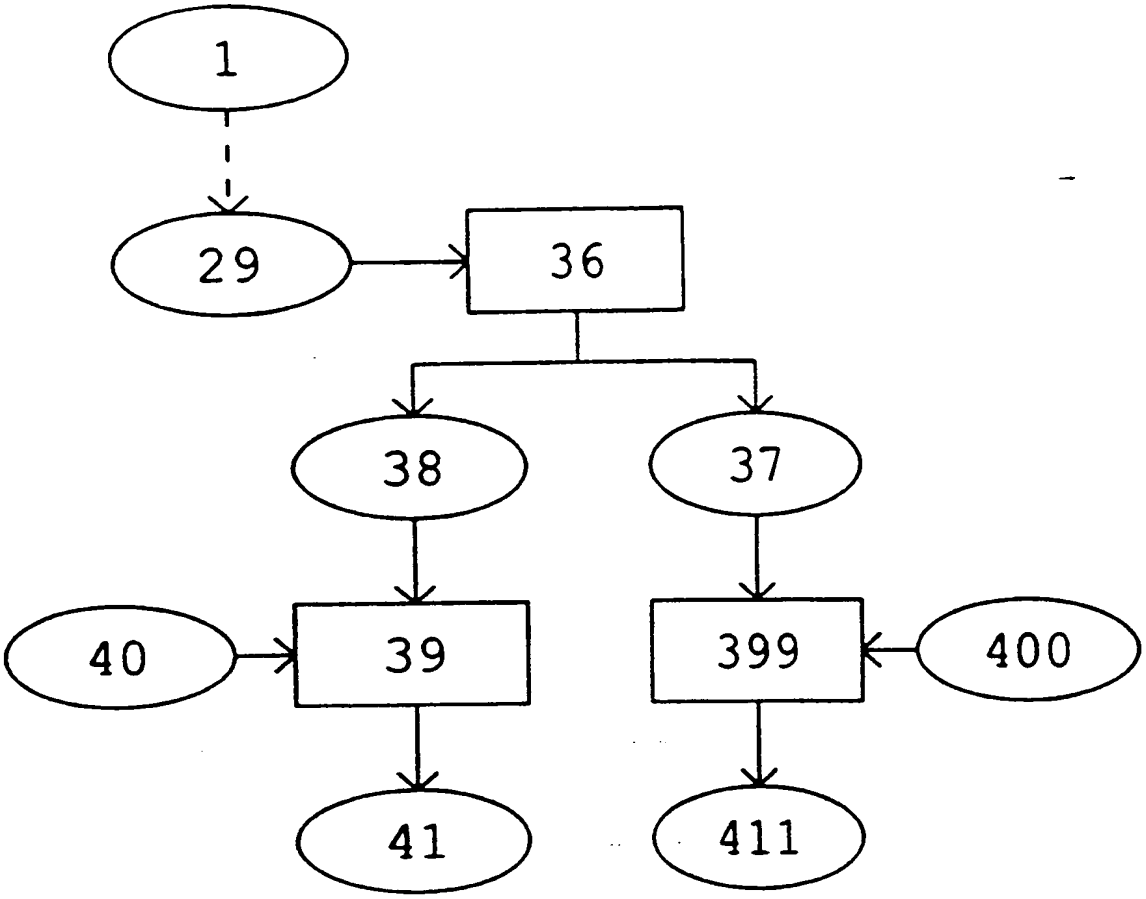


FIG. 7

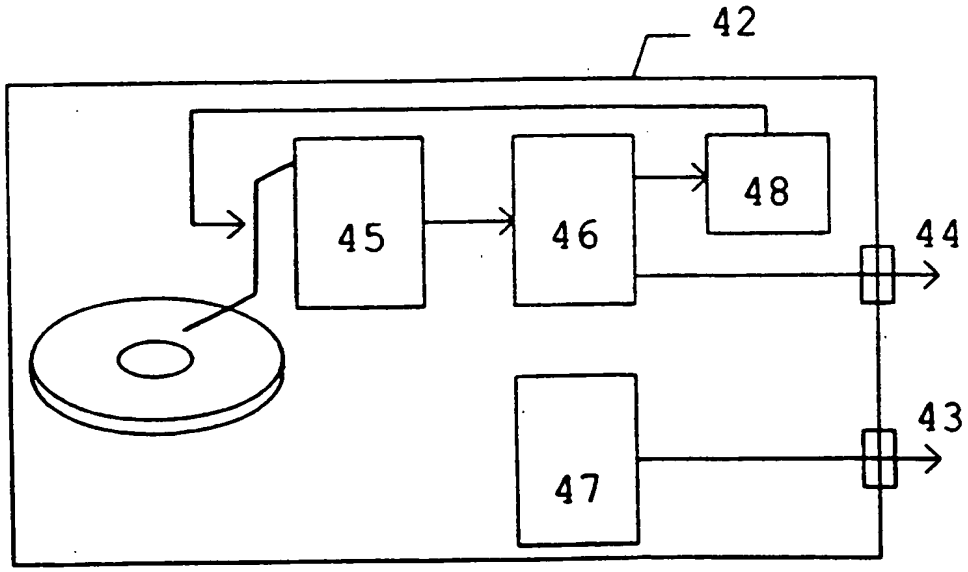


FIG. 8

INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/FR 99/02267

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 413 350 A (TOKYO SHIBAURA ELECTRIC CO) 20 February 1991 (1991-02-20) abstract column 2, line 30 -column 3, line 25 column 5, line 23 -column 9, line 5 figures 1-4 ---	1-5,10
A	US 4 937 679 A (RYAN JOHN O) 26 June 1990 (1990-06-26) abstract; figure 1 column 3, line 2 - line 60 ---	1,10
A	EP 0 416 663 A (MATSUSHITA ELECTRIC IND CO LTD) 13 March 1991 (1991-03-13) abstract column 4, line 40 -column 5, line 13 claims 1,3; figure 2 --- -/--	1,5-7,10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 1999	12/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schiwy-Rausch, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/FR 99/02267

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0413350 A	20-02-1991	JP 1861103 C	08-08-1994
		JP 3075827 A	29-03-1991
		JP 5070176 B	04-10-1993
		DE 69032305 D	18-06-1998
		DE 69032305 T	08-10-1998
		US 5295187 A	15-03-1994
US 4937679 A	26-06-1990	US 5130810 A	14-07-1992
		AT 122835 T	15-06-1995
		DE 68922658 D	22-06-1995
		DE 68922658 T	19-10-1995
		EP 0348218 A	27-12-1989
		ES 2072300 T	16-07-1995
		HK 1002419 A	21-08-1998
		JP 2064947 A	05-03-1990
		KR 9406160 B	08-07-1994
		PH 26068 A	29-01-1992
		AT 96933 T	15-11-1993
		DE 3788020 D	09-12-1993
		DE 3788020 T	03-03-1994
		EP 0256753 A	24-02-1988
		ES 2044937 T	16-01-1994
		HK 1008109 A	30-04-1999
		IE 62247 B	11-01-1995
		JP 2881432 B	12-04-1999
		JP 63107281 A	12-05-1988
		US 4907093 A	06-03-1990
		US 4819098 A	04-04-1989
		US 5194965 A	16-03-1993
EP 0416663 A	13-03-1991	JP 2629372 B	09-07-1997
		JP 3097167 A	23-04-1991
		JP 2584067 B	19-02-1997
		JP 3102676 A	30-04-1991
		DE 69032036 D	19-03-1998
		DE 69032036 T	20-08-1998
		KR 9408688 B	24-09-1994
		US 5159502 A	27-10-1992
EP 0735752 A	02-10-1996	JP 8275127 A	18-10-1996
		AU 709546 B	02-09-1999
		AU 4826396 A	10-10-1996
		BR 9601234 A	06-01-1998
		CA 2172009 A	01-10-1996
		CN 1135142 A	06-11-1996
		US 5778064 A	07-07-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Dem : Internationale No
PCT/FR 99/02267

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultee (système de classification suivi des symboles de classement)
CIB 7 G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 413 350 A (TOKYO SHIBAURA ELECTRIC CO) 20 février 1991 (1991-02-20) abrégé colonne 2, ligne 30 -colonne 3, ligne 25 colonne 5, ligne 23 -colonne 9, ligne 5 figures 1-4	1-5,10
A	US 4 937 679 A (RYAN JOHN O) 26 juin 1990 (1990-06-26) abrégé; figure 1 colonne 3, ligne 2 - ligne 60	1,10
A	EP 0 416 663 A (MATSUSHITA ELECTRIC IND CO LTD) 13 mars 1991 (1991-03-13) abrégé colonne 4, ligne 40 -colonne 5, ligne 13 revendications 1,3; figure 2	1,5-7,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 novembre 1999	12/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schiwy-Rausch, G

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 99/02267

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0413350 A	20-02-1991	JP 1861103 C	08-08-1994
		JP 3075827 A	29-03-1991
		JP 5070176 B	04-10-1993
		DE 69032305 D	18-06-1998
		DE 69032305 T	08-10-1998
		US 5295187 A	15-03-1994
US 4937679 A	26-06-1990	US 5130810 A	14-07-1992
		AT 122835 T	15-06-1995
		DE 68922658 D	22-06-1995
		DE 68922658 T	19-10-1995
		EP 0348218 A	27-12-1989
		ES 2072300 T	16-07-1995
		HK 1002419 A	21-08-1998
		JP 2064947 A	05-03-1990
		KR 9406160 B	08-07-1994
		PH 26068 A	29-01-1992
		AT 96933 T	15-11-1993
		DE 3788020 D	09-12-1993
		DE 3788020 T	03-03-1994
		EP 0256753 A	24-02-1988
		ES 2044937 T	16-01-1994
		HK 1008109 A	30-04-1999
		IE 62247 B	11-01-1995
		JP 2881432 B	12-04-1999
		JP 63107281 A	12-05-1988
		US 4907093 A	06-03-1990
		US 4819098 A	04-04-1989
		US 5194965 A	16-03-1993
EP 0416663 A	13-03-1991	JP 2629372 B	09-07-1997
		JP 3097167 A	23-04-1991
		JP 2584067 B	19-02-1997
		JP 3102676 A	30-04-1991
		DE 69032036 D	19-03-1998
		DE 69032036 T	20-08-1998
		KR 9408688 B	24-09-1994
		US 5159502 A	27-10-1992
EP 0735752 A	02-10-1996	JP 8275127 A	18-10-1996
		AU 709546 B	02-09-1999
		AU 4826396 A	10-10-1996
		BR 9601234 A	06-01-1998
		CA 2172009 A	01-10-1996
		CN 1135142 A	06-11-1996
		US 5778064 A	07-07-1998

PROTECTION AGAINST THE COPYING OF DIGITAL DATA STORED ON AN INFORMATION CARRIER

The invention relates to a method and a device making it possible to protect against the copying of digital data stored on an information carrier.

A possibility inherent in digital data is that they can be copied without appreciable loss of quality since copying consists in transmitting a series of "1"s and "0"s from the source to the recorder. The greatest number of errors which may occur when copying can be countered by using error correction methods. Thus, when an information carrier contains digital data, it is in principle relatively simple to record the content of the information carrier identically on a recordable carrier.

Numerous types and kinds of information carriers are used to store information of all sorts in digital form. For example, a magnetic tape, a recordable or non-recordable optical disk (CD, CD-R, CD-RW, DVD, DVD-R, magneto-optical disk, etc., respectively standing for Compact Disk, CD-Recordable, CD-Read Write, Digital Versatile Disk, DVD-Recordable) can store audio and/or video information in digital form.

In order to better safeguard for example the interests of the authors of stored information or those of producers of prerecorded information carriers, it is desirable to limit the possibilities of freely and simply copying the digital data. Various mechanisms and possibilities currently exist for protecting digital data against illegitimate copying.

In a known manner, the digital data can be encrypted when they are stored on the information carrier. Encryption makes it possible to limit the use of the digital data to the holder of a public or private deencryptioning key. Encryption is for example used in the protection of data on DVDs, optical disks used to store video data in digital form. Thus, a DVD

player requires an appropriate key in order to decrypt the data read from the DVD.

One way of protecting digital data against copying consists in furnishing them with a watermark, that is to say with auxiliary data attached to the digital data. The watermark must be unmodifiable and non-erasable. The playing of the data is carried out with the aid of a public key which identifies the watermark. The public key is a code well known to the public, or more precisely contained in most players of information carriers. Should the watermarked digital data be copied, a private key is required in order to put the watermark back in place on the copy, failing which the copy becomes illegal devoid as it is of watermark. The private key is held by the author or the producer of the information thus watermarked. The digital data copied without watermark are no longer played by the player since the latter does not identify any watermark where it ought to find one. Thus, the watermark precludes copying without the private key. If a copy is necessary then the recorder must build in this private key.

Watermarking does not prevent the copying of the digital data by an analog route, that is to say copying which would firstly require conversion of the digital data into an analog signal and which would take the analog signal as the source of the copy.

A known solution for preventing the copying of a digital carrier by an analog route and more particularly in the field of video and television consists in corrupting the analog signal in such a way that it can be used to display an image on the screen of a television set by way of an analog input of this television set, but so that the same signal cannot be used to make a copy with a video recorder. More precisely, an electronic circuit is employed to influence image synchronization parameters. These synchronization parameters are perceived differently by a television set and by a video recorder. This solution

does not make it possible to prevent the digital copying of digital data.

Another solution for limiting digital copies of digital data consists in furnishing the latter with copy generation management information. In principle, this information item conveys the information item "never copy" for data which do not have the right to be copied and the information item "copy" or "copy number X" if the data are a first generation or X-th generation copy of an original. Thus, a recorder can, with the aid of these information items, ascertain whether the digital data to be copied have the right to be copied digitally and prevent copying if it is prohibited for the 2nd or (X+1th) generation. The copy generation management information item is updated with each copy. This manipulation of the copy generation management information item renders it vulnerable to falsification. Specifically, the copy generation management information item is at one stage of copying available as plaintext, that is to say in decrypted form. The manipulation also requires the digital recorder to be equipped accordingly. The copy generation management information item does not by itself make it possible to prevent copying by an analog route.

An object of the invention consists in finding a solution for protection against digital copying in which no information item relating to the generation of copy is available as plaintext when copying.

Another object of the invention consists in finding a solution in which no modification of data relating to protection against copying is undertaken upon the possible recording of a copy.

A solution proposed by the invention envisages a method of protection against the copying of digital data stored on an information carrier, comprising

a first identification of an encryption of the digital data,

a second identification of a watermarking of digital data,

a first determination of a first mark if it has been possible to identify the encryption and the watermarking,

a third identification of a type of the information carrier,

a second determination of a second mark if it has been possible to determine the first mark and if it has been possible to identify a determined type of information carrier,

a fourth identification of cryptographic signature data accompanying the digital data,

a third determination of a third mark if it has been possible to determine the second mark and if it has been possible to identify a cryptographic signature datum,

a first delivery of a permission for digital copying of the digital data if it has been possible to determine the third mark.

A first advantageous implementation of the invention envisages a second delivery of a prohibition of playing of the digital data if the first identification is negative and if it has been possible to identify the watermarking, or if it has been possible to identify the encryption and the second identification is negative.

A second advantageous implementation of the invention envisages a third delivery of a permission for digital copying of the digital data if the first and second identifications are negative.

A third advantageous implementation of the invention envisages a fourth delivery of a prohibition of digital copying of the digital data if it has been possible to determine the first mark and if the third identification reveals a different type from the determined type of information carrier.

A fourth advantageous implementation of the invention envisages a fifth delivery of a prohibition

of digital copying of the digital data if it has been possible to determine the second mark and if the fourth identification is negative.

A fifth advantageous implementation of the invention envisages a conversion of the digital data into analog signals and a corruption of the analog signals if the first, the fourth or the fifth delivery has been implemented.

A sixth advantageous implementation of the invention envisages that the prohibition of digital copying comprises a blocking of output of the digital data.

A seventh advantageous implementation of the invention envisages a deencryptioning of the digital data if it has been possible to identify a encryption so as to obtain decrypted digital data and decrypted cryptographic signature data, and a first encryption of the cryptographic signature data with the aid of a public key.

Another solution proposed by the invention envisages a device for playing digital data stored on an information carrier comprising at least,

a digital output for providing signals representative of the digital data upon playing the digital data,

an analog output for providing analog signals representative of the digital data upon playing the digital data,

a decryption system for the digital data making it possible in particular to establish whether the digital data are encrypted and, if so, to decryption the encrypted digital data, to identify whether the digital data comprise a watermark and/or cryptographic signature data, and to identify a type of the information carrier,

a system for protection against the copying of digital data receiving signals from the decryption system so as to evaluate them, and generating a copy permission signal in the case where the digital data

are encrypted, have a watermark, are on a carrier of non-recordable type and possess cryptographic signature data,

a recording control part for managing a stream of digital data heading for the digital output when it receives in particular a copy permission signal,

a playing protection system, receiving signals from the decryption system and generating a playing prohibition signal when the digital data are not encrypted but watermarked, or when the digital data are encrypted but not watermarked,

a playing control part for interrupting the playing of the data or their output to the analog output when it receives in particular a playing prohibition signal.

In what follows, exemplary implementations are presented which will illustrate the invention and provide a better understanding thereof, while referring to figures 1 to 8, briefly described hereinbelow:

Fig. 1 contains a flowchart illustrating an embodiment of the invention,

Figs. 2 to 5 contain flowcharts illustrating aspects of the invention,

Fig. 6 contains a flowchart illustrating a digital/analog conversion according to the invention,

Fig. 7 contains a flowchart illustrating aspects of the invention which relate to the encryption,

Fig. 8 contains a diagram illustrating a device according to the invention.

Fig. 1 contains a flowchart in which digital data stored on an information carrier 1 are subjected to a first identification of an encryption 2 so as to verify whether the digital data are stored in encrypted form, then to a second identification of a watermark 3 so as to see whether the data are provided with a digital watermark. A first bifurcation 4 makes it possible to distinguish the cases in which an encryption is identified 5 or not 6. A second bifurcation 7 makes it possible to distinguish the cases in which a watermark

is identified 8 or not 9. If cases 5 and 8 are indeed verified, a first determination 10 generates a first mark #1.

A third identification 11 of a type of the information carrier 1 serves to see whether the information carrier is for example of the non-recordable or recordable type. An information item regarding the type can be contained in the digital data per se or result from physical measurements of parameters of the information carrier 1 during for example installation in a player of the information carrier 1. A third bifurcation 12 makes it possible to distinguish the cases in which the type might be a determined type 13, for example a non-recordable information carrier such as a pressed optical disk, or not 14. If case 13 is indeed verified and the first mark #1 has been generated, then a second determination 15 generates a second mark #2.

A fourth identification 16 of cryptographic signature data verifies whether the digital data possess a cryptographic signature. A fourth bifurcation 17 makes it possible to distinguish the cases in which the cryptographic signature is present 18 or not 19. If case 18 is indeed verified and the second mark #2 has been generated, then a third determination 20 generates a third mark #3.

In the presence of the third mark #3, a first delivery 21 of permission for digital copying 22 of the digital data is implemented.

Overall, the flowchart of Fig. 1 shows how various criteria pertaining to the digital data and also to the information carrier can lead to the delivery of permission for digital copying, the idea being to allow copying only under defined conditions. For example, the data should not have been manipulated and hence should be encrypted and watermarked. Next, the data should not yet have been copied. If the data are on a non-recordable disk then a priori the data are on an original information carrier. Finally, the data should

possess a cryptographic signature. The latter indicates that the data can be copied. It is then that the data receive the permission for digital copying. A result of the copying of the data will be identical to the original except as regards the information carrier which will have to be recordable. A new copy of the data from the recordable information carrier would be impossible since the second mark #2 could not be generated after the third identification 11. Specifically, the third bifurcation 12 would lead us to case 14.

Other exemplary cases need to be considered when for example the encryption or the watermarking of the digital data cannot be identified. Normally, encryption and watermarking go hand in hand and the absence of one or the other is evidence of illicit manipulation of the digital data. It is then necessary to go further than simply prohibiting the copying of the digital data. The playing of the latter must be prevented.

A flowchart in Fig. 2 illustrates two exemplary cases in which the encryption and the watermarking are not identified together. An exemplary case envisages that the first bifurcation 4 yields case 6, that is to say that the first identification of an encryption is negative, and that the second bifurcation 7 yields case 8, that is to say that a watermark is present. Then a second delivery 23 generates a prohibition of playing of the digital data 24. In practice, this could for example lead to an interruption of the playing of the data. Another exemplary case envisages that the first bifurcation 4 yields case 5, that is to say an encryption is identified, and that the second bifurcation 7 yields case 9, that is to say that the second identification of a watermark is negative. In this other case the second delivery generates the prohibition of playing 24.

The method described allows to freely copy digital data which are not protected, for example data devoid of encryption and of watermark. Fig. 3 contains a

flowchart in which the first and the second bifurcation 4 and 7 each yield a case of negative identification respectively cases 6 in respect of encryption and 9 in respect of watermark. A third delivery 25 then directly generates the digital copying permission 22.

In the last case it matters little whether the data are on a recordable or non-recordable information carrier. The absence of encryption and of watermark indicates a minimum level of data protection.

In certain exemplary cases it has to be possible to play and utilize the data but not to copy them. This is the case in particular when one purchases an information carrier containing digital data, the copying of which the author or the producer wishes to prevent. This is also the case when a recordable information carrier containing legally copied data is played. Such a case is illustrated with the aid of a flowchart in Fig. 4 where a fourth delivery 26 verifies that the first mark #1 has been delivered and that case 14 of identification of a type of information carrier different from the determined type has occurred before generating a prohibition of copying 27. In practice, the player would have to employ a device preventing copying of the digital data, for example by disabling a digital output of the player.

Another such case is illustrated with the aid of a flowchart in Fig. 5. If the second mark #2 is identified and case 19 signals a fourth negative identification, that is to say that no cryptographic signature permitting copying of the data is present, then a fifth delivery 28 generates the prohibition of copying 27.

Of course the fact that no cryptographic signature permitting copying of the data is identified does not exclude the presence of a particular cryptographic signature prohibiting copying.

Throughout the description, mention has already been made of the fact that the information carrier 1 is used in an appropriate player. The digital data stored

on the information carrier 1 can in certain cases be conveyed to a digital output of the player. In the example of a DVD (optical disk for video/audio digital data) player, a digital output can be provided in order to output a signal representative of the data to a DVD-R (or other) player/recorder for copying purposes, or to a computer to carry out image processing. In general, the player also provides an analog output so as to be able to transmit an analog signal representative of the digital data to the analog input for example of a television set.

A flowchart in Fig. 6 indicates with a dashed arrow that the information carrier yields digital data 29. A conversion 30 makes it possible to convert the digital data 29 into analog signals 31. A presence of the permission for digital copying 22 together with any one of the first, second or third marks (#1, #2, #3), or a presence of the prohibition of digital copying 27, is detected in a detection 32 which as appropriate triggers a corruption 33 of the analog signals so as to obtain corrupted analog signals 34. The analog signals are for example corrupted in such a way that they can be used to obtain images on a television but that it is impossible to copy them with the aid of a video recorder with an analog input.

Advantageously there is envisaged a blocking at a digital output of the player of the digital data 35 in the presence of the prohibition of digital copying 27.

The encryption of the digital data on the information carrier is normally performed on the producer side. Encryption is performed with the aid of an encryption algorithm and of a private key held only by the producer. The encryption is designed in such a way that it is possible to decrypt the data with the aid of a widely available public key. When decrypting the data, the part relating to the cryptographic signature is of course also decrypted and needs to be re-encrypted without however being modified before being transmitted to a digital output for copying. In

order to limit the risk of the pirating of a private key, the player does not contain this private key and re-encrypts the cryptographic signature with the aid of a public key. Fig. 7 contains a flowchart in which the information carrier 1 is a source of digital data 29. Decryption 36 makes it possible to obtain decrypted digital data 37 and in particular a decrypted cryptographic signature 38. The latter is encrypted during a first encryption 38 with the aid of a public key 40 contained in the player before being conveyed in the form of an encrypted cryptographic signature 41 to a digital output (not illustrated) together with the encrypted digital data 411 encrypted during a second encryption 399 with the aid of the private key 400. Thus, no manipulation of the data and of the watermark is possible.

A device for playing digital data 42 in Fig. 8, comprises a digital output 43 which provides signals representative of the digital data upon playing the digital data of an information carrier. This output 43 can for example be implemented with the aid of a digital bus to the IEEE1394 standard. An analog output 44 provides analog signals representative of the same digital data. A decryption system 45 makes it possible to decrypt digital data if the latter are encrypted, but also to identify any watermark and cryptographic signature data. The decryption system makes it possible to accomplish for example the identifications 2, 3, 11 and 16 of the method illustrated in Fig. 1.

A protection system in respect of the copying of the digital data 46 uses signals transmitted by the decryption system 45 and evaluates them by implementing the determinations 10, 15 and 20 of the method illustrated in Fig. 1 and delivers, after having determined the marks #1, #2 and #3, a copy permission signal.

A recording control part 47 manages a stream of digital data heading for the digital output. This part, when it obtains the copy permission signal from the

protection system 46, can in particular activate the stream.

The protection system in respect of the copying of the digital data 46 can also play the role of a playing protection system. With the aid of the signals received from the decryption system 45, the latter system generates a playing prohibition signal when the digital data are not encrypted but watermarked or else when the digital data are encrypted but not watermarked.

A playing control 48 makes it possible to interrupt the playing of the digital data when it receives the prohibition signal from the playing protection system.

List of references

1 information carrier
2 first identification of an encryption
3 second identification of a watermark
4 first bifurcation
5 encryption identified
6 encryption not identified
7 second bifurcation
8 watermark identified
9 watermark not identified
10 first determination
#1 first mark
11 third identification of a type of information carrier
12 fourth bifurcation
13 determined type
14 not the determined type
15 second determination
#2 second mark
16 fourth identification of cryptographic signature data
17 fourth bifurcation
18 cryptographic signature present
19 cryptographic signature not present
20 third determination
#3 third mark
21 first delivery
22 permission for digital copying
23 second delivery
24 prohibition of playing digital data
25 third delivery
26 fourth delivery
27 prohibition of copying
28 fifth delivery
29 digital data
30 conversion
31 analog signals
32 detection

33 corruption
34 corrupted analog signals
35 digital data output suppression
36 decryption of digital data
37 decrypted digital data
38 decrypted cryptographic signature data
39 first encryption
399 second encryption
40 public key
41 encrypted cryptographic signature
411 encrypted digital data
42 digital data playing device
43 digital output
44 analog output
45 decryption system
46 protection system in respect of the copying of digital data
47 recording control part
48 playing control part

Claims

1. A method of protection against the copying of digital data stored on an information carrier (1), comprising

a first identification of an encryption (2) of the digital data,

a second identification of a watermarking (3) of the digital data,

characterized in that the method furthermore comprises

a first determination (10) of a first mark (#1) if it has been possible to identify (5, 8) the encryption and the watermarking,

a third identification of a type of the information carrier (11),

a second determination (15) of a second mark (#2) if it has been possible to determine the first mark (#1) and if it has been possible to identify (13) a determined type of information carrier,

a fourth identification of cryptographic signature data (16) accompanying the digital data,

a third determination (20) of a third mark (#3) if it has been possible to determine the second mark (#2) and if it has been possible to identify (18) a cryptographic signature datum,

a first delivery (21) of a permission for digital copying (22) of the digital data if it has been possible to determine the third mark (#3).

2. The method of protection as claimed in claim 1, characterized in that it comprises

a second delivery (23) of a prohibition of playing (24) of the digital data if the first identification is negative (6) and if it has been possible to identify (8) the watermarking, or if it has been possible to identify (5) the encryption and the second identification is negative (9).

3. The method of protection as claimed in either of claims 1 or 2, characterized in that it comprises

a third delivery (25) of a permission for digital copying (22) of the digital data if the first (6) and second (9) identifications are negative.

4. The method of protection according to any one of claims 1 to 3, characterized in that it comprises

a fourth delivery (26) of a prohibition of digital copying (27) of the digital data if it has been possible to determine the first mark (#1) and if the third identification reveals a different type (14) from the determined type of information carrier.

5. The method of protection as claimed in any one of claims 1 to 4, characterized in that it comprises

a fifth delivery (28) of a prohibition of digital copying (27) of the digital data if it has been possible to determine the second mark (#2) and if the fourth identification is negative (19).

6. The method of protection as claimed in any one of claims 1, 4 or 5, characterized in that it comprises

a conversion (30) of the digital data (29) into analog signals (31),

a corruption (33) of the analog signals if the first (21), the fourth (26) or the fifth delivery (28) has been implemented.

7. The method of protection as claimed in either of claims 4 or 5, characterized in that the prohibition of digital copying (27) comprises a blocking (35) of output of the digital data.

8. The method of protection as claimed in claim 1, characterized in that it comprises

a decryption of the digital data (36) if it has been possible to identify an encryption so as to obtain decrypted digital data (37) and decrypted cryptographic signature data (38),

a first encryption (39) of the cryptographic signature data with the aid of a public key (40).

9. The method of protection as claimed in claim 8, characterized in that it comprises

a second encryption (399) of the decrypted digital data with the aid of a private key (400).

10.A device for playing digital data stored on an information carrier comprising at least,

a digital output (43) for providing signals representative of the digital data upon playing the digital data,

an analog output (44) for providing analog signals representative of the digital data upon playing the digital data,

a decryption system (45) for the digital data making it possible in particular to establish whether the digital data are encrypted and, if so, to decrypt the encrypted digital data, to identify whether the digital data comprise a watermark and/or cryptographic signature data, and to identify a type of the information carrier,

a system (46) for protection against the copying of digital data receiving signals from the decryption system so as to evaluate them, and generating a copy permission signal in the case where the digital data are encrypted, have a watermark, are on a carrier of non-recordable type and possess cryptographic signature data,

a recording control part (47) for managing a stream of digital data heading for the digital output when it receives in particular a copy permission signal,

a playing protection system, receiving signals from the decryption system and generating a playing prohibition signal when the digital data are not encrypted but watermarked, or when the digital data are encrypted but not watermarked,

a playing control part (48) for interrupting the playing of the data or their output to the analog

output when it receives in particular a playing prohibition signal.

ABSTRACT

PROTECTION AGAINST THE COPYING OF DIGITAL DATA STORED ON AN INFORMATION CARRIER

A method of protection against the copying of digital data stored on an information carrier (1) envisages, on the basis of a first identification of an encryption (2) of the digital data and of a second identification of a watermarking (3) of digital data, the determination (10) of a first mark (#1) if it has been possible to identify (5, 8) the encryption and the watermarking. A third identification of a type of the information carrier (11) is followed by the determination (15) of a second mark (#2) if it has been possible to determine the first mark (#1) and if it has been possible to identify (13) a determined type of information carrier. A fourth identification of cryptographic signature data (16) accompanying the digital data is followed by the determination (20) of a third mark (#3) if it has been possible to determine the second mark (#2) and if it has been possible to identify (18) a cryptographic signature datum. A permission for digital copying (22) of the digital data is delivered if it has been possible to determine the third mark (#3).

FIG. 1

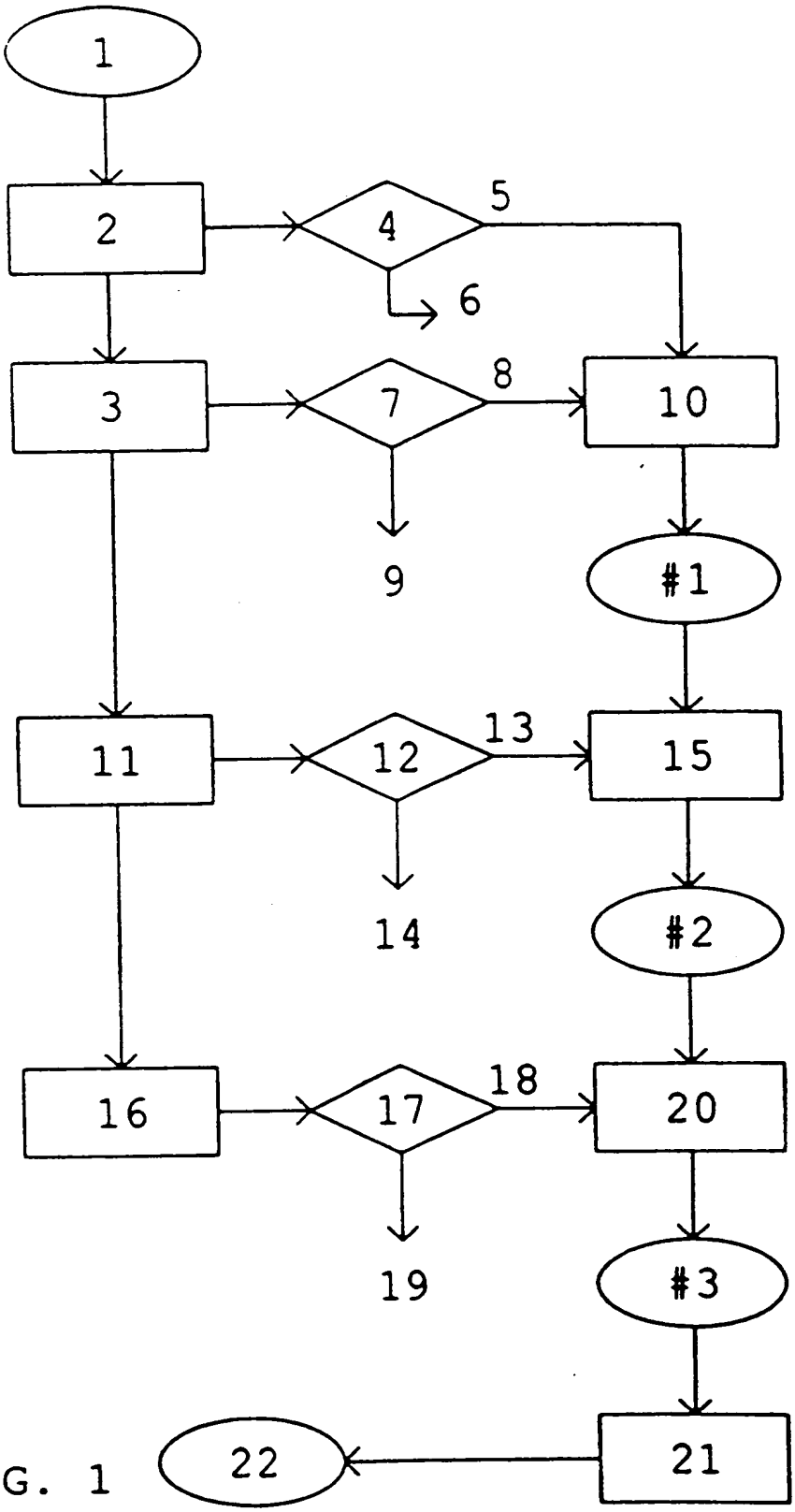


FIG. 1

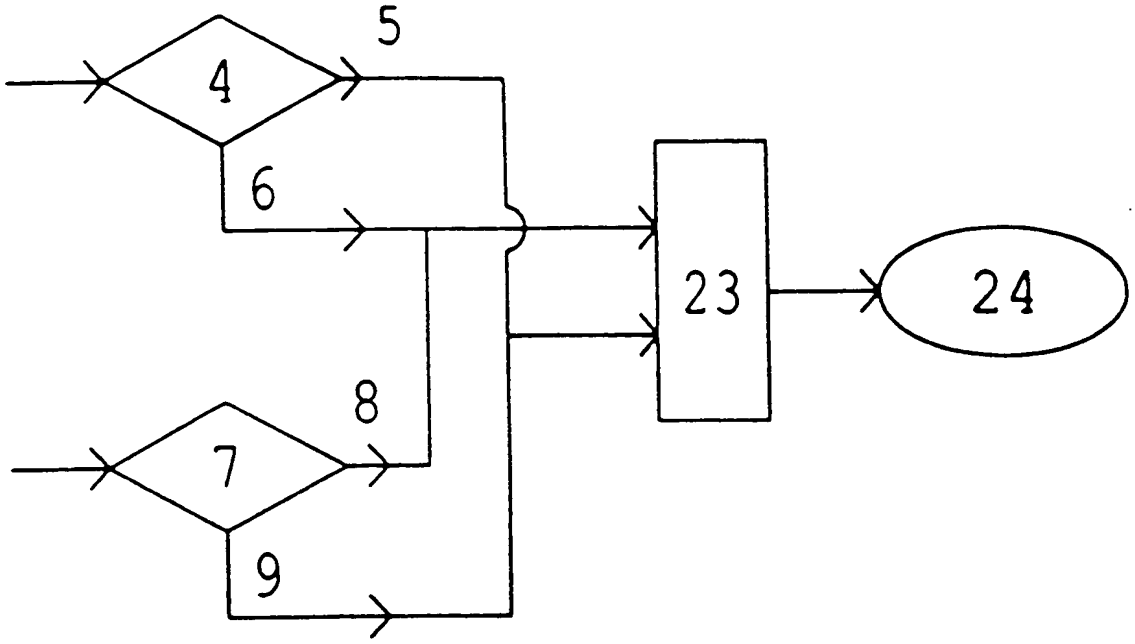


FIG. 2

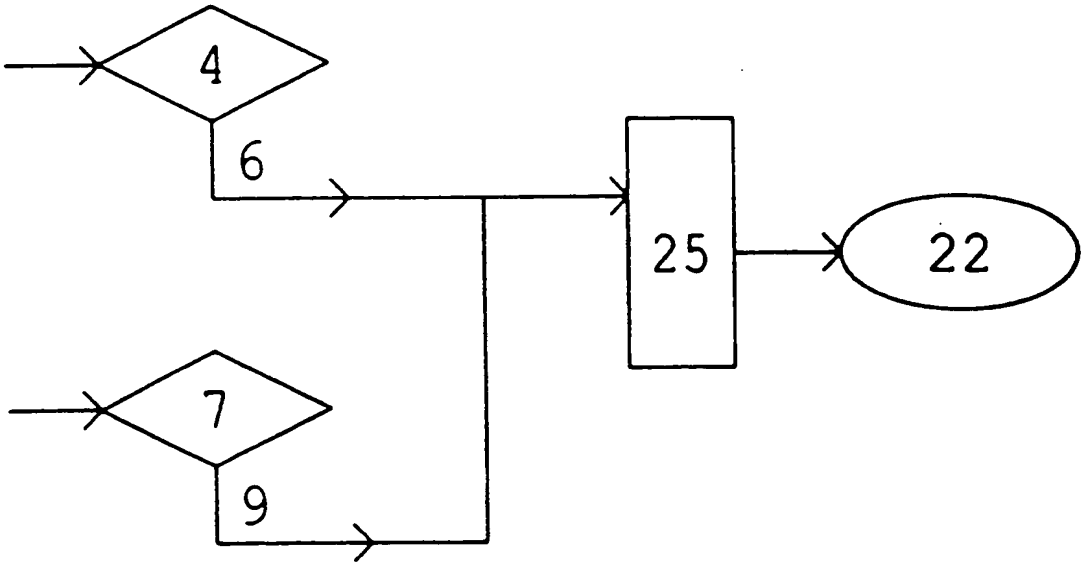


FIG. 3

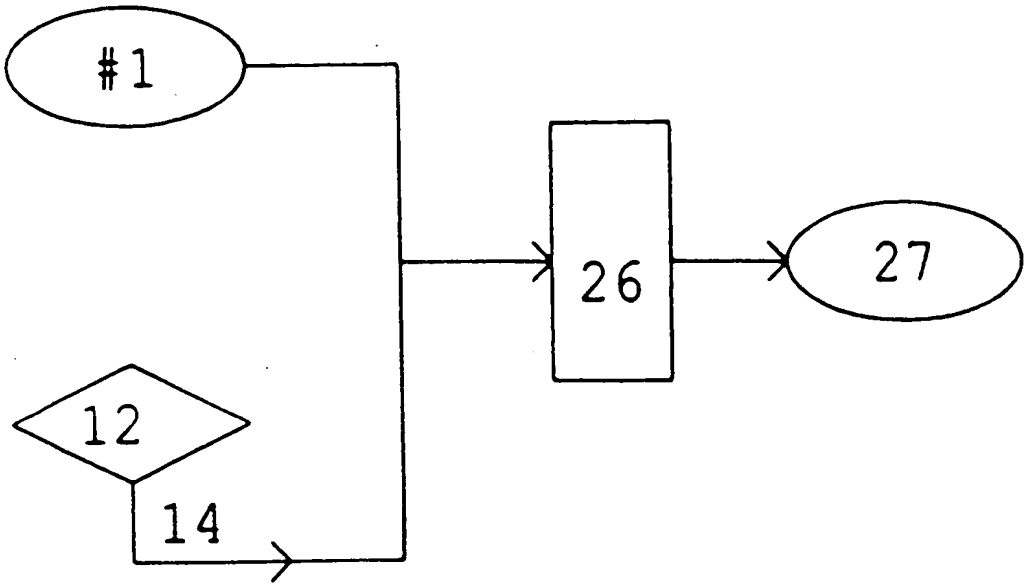


FIG. 4

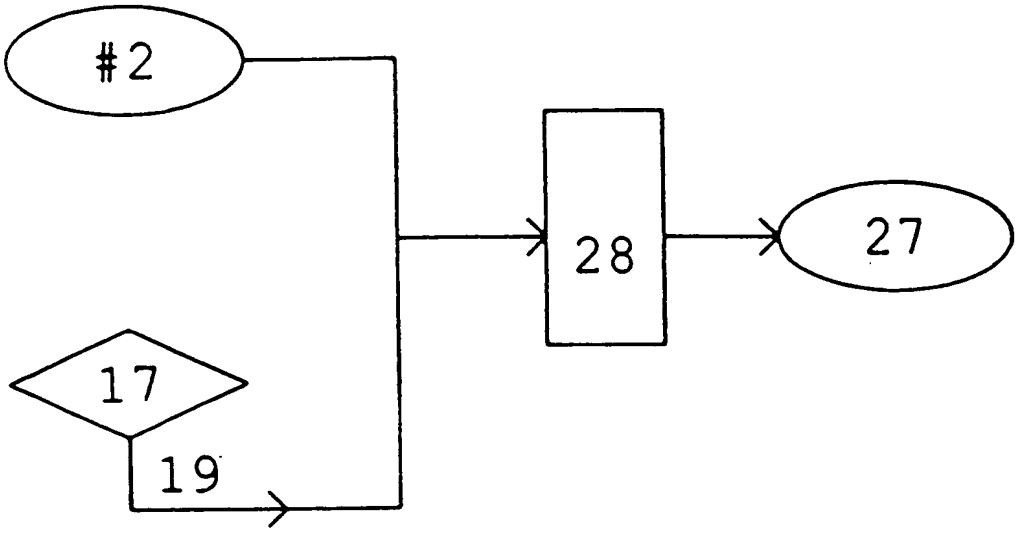


FIG. 5

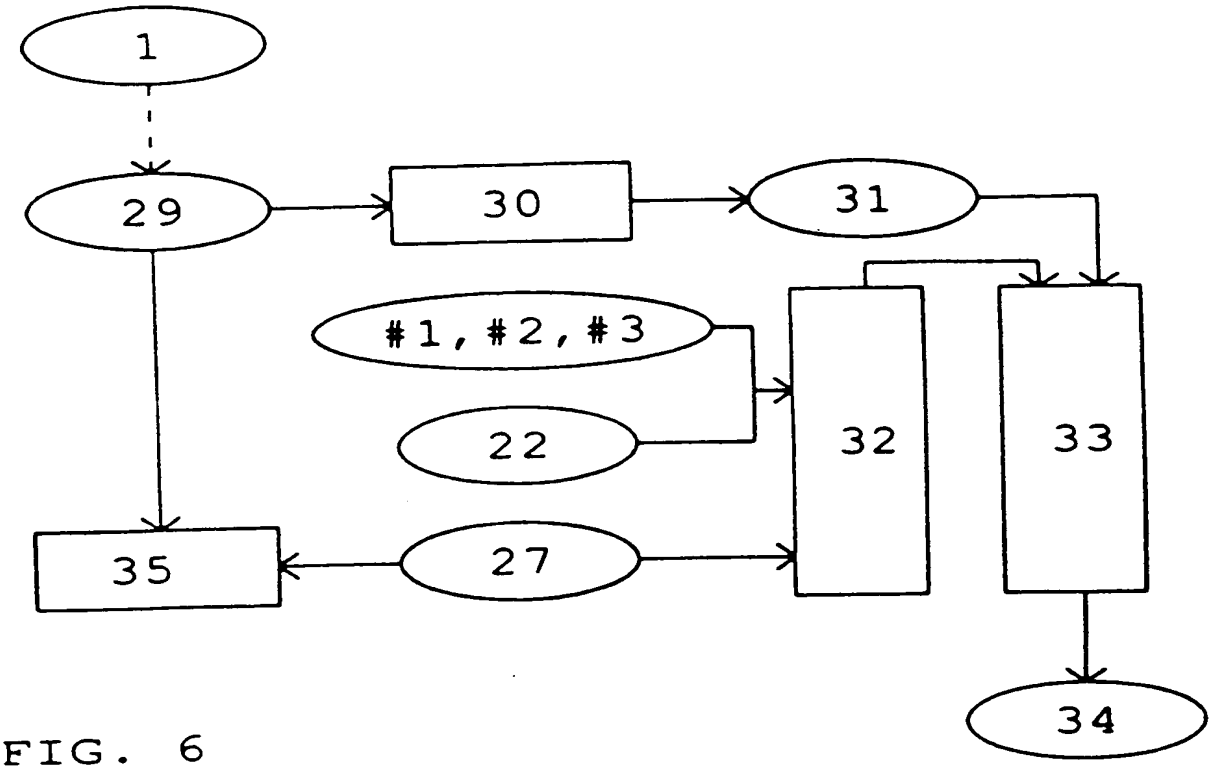


FIG. 6

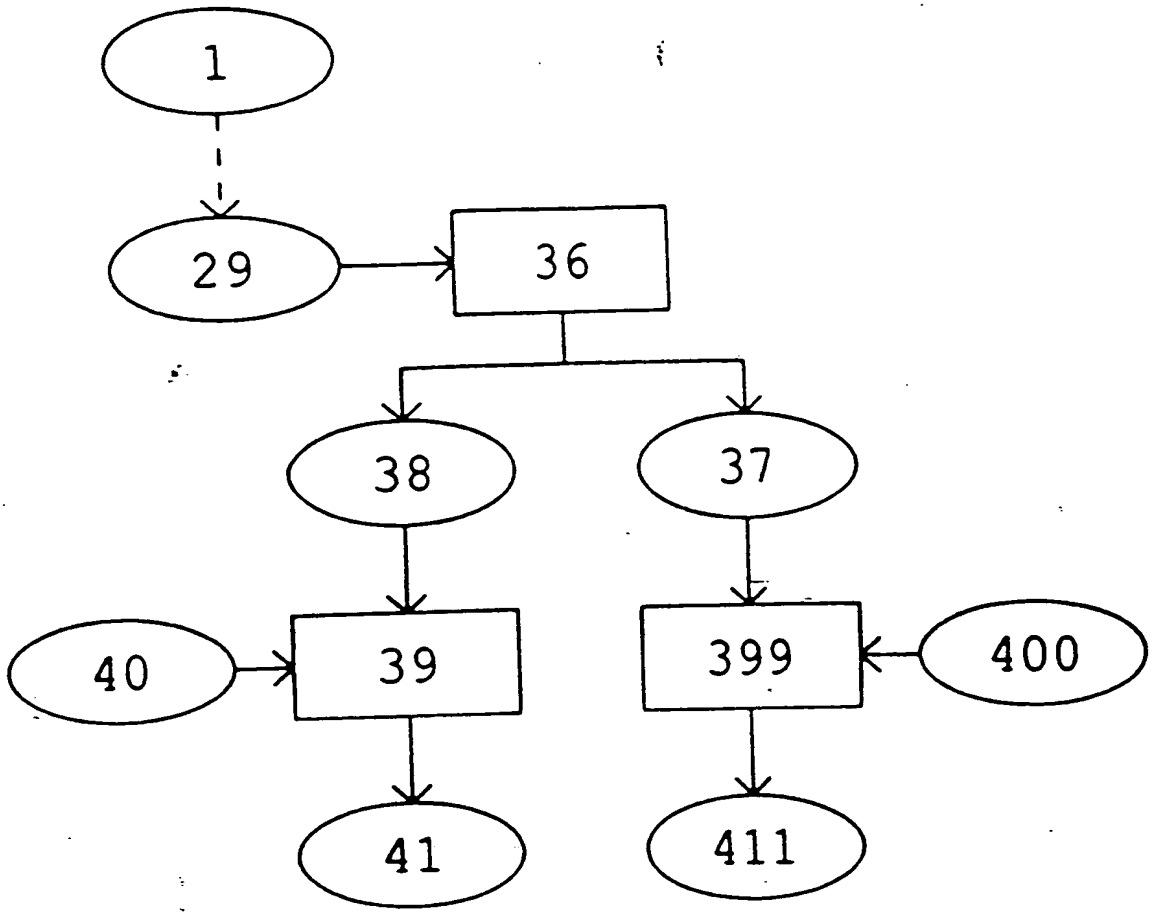


FIG. 7

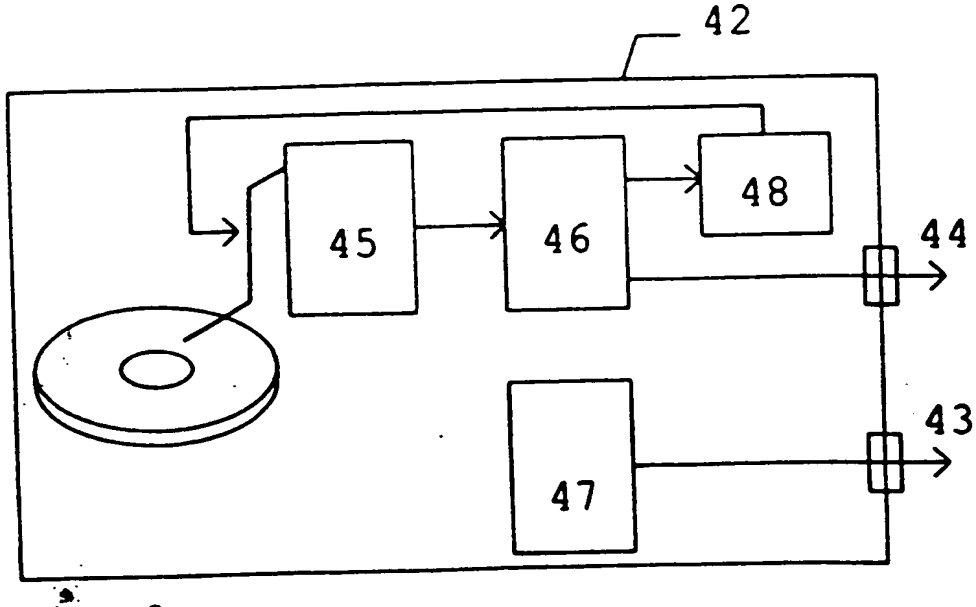


FIG. 8

TRAITE DE COOPERATION EN MATIERE DE BREVETS

EXPRESS MAIL EL682441985US

Expéditeur: L'ADMINISTRATION CHARGEE DE L'EXAMEN PRELIMINAIRE INTERNATIONAL

THOMSON multimedia RECEIVED 10 NOV. 2000 Patent Department Administration

PCT

Destinataire:

KOHRS, M.
THOMSON MULTIMEDIA
46 Quai Alphonse Le Gallo
F-92648 Boulogne Cedex
FRANCE

NOTIFICATION DE TRANSMISSION DU RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(règle 71.1 du PCT)

Date d'expédition *(jour/mois/année)*	08.11.2000
Référence du dossier du déposant ou du mandataire: PF980065	**NOTIFICATION IMPORTANTE**

Demande internationale No.	Date du dépot international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR99/02267	23/09/1999	23/09/1998

Déposant: THOMSON MULTIMEDIA et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. **RAPPEL**

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Losrqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international	Fonctionnaire autorisé
Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Slater, S Tél.+49 89 2399-2565

Formulaire PCT/IPEA/416 (juillet 1992)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire PF980065	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02267	Date du dépot international *(jour/mois/année)* 23/09/1999	Date de priorité *(jour/mois/année)* 23/09/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G11B20/00		
Déposant THOMSON MULTIMEDIA et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 16 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
11/04/2000	08.11.2000
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Sucher, R N° de téléphone +49 89 2399 2148

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02267

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

Description, pages:

2,10	version initiale	
1,3-9,11	reçue(s) avec télécopie du	20/10/2000

Revendications, N°:

1-9	reçue(s) avec télécopie du	20/10/2000

Dessins, feuilles:

1/4-4/4	reçue(s) avec télécopie du	20/10/2000

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   - ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   - ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   - ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   - ☐ contenu dans la demande internationale, sous forme écrite.
   - ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   - ☐ remis ultérieurement à l'administration, sous forme écrite.
   - ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   - ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   - ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, n^{os} :

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-9
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-9
Possibilité d'application industrielle	Oui :	Revendications	1-9
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence aux documents suivants:

   D1: WO-A-9733283 (TIME WARNER ENTERTAINMENT CO) 1997-09-12;
   D2: WO-A-9600963 (MACROVISION CORP) 1996-01-11;
   D3: EP-A-0 413 350 (TOKYO SHIBAURA ELECTRIC CO) 1991-02-20.

   Les documents D1 et D2 n'ont pas été cités dans le rapport de recherche international.

2. Selon la description, les caractéristiques suivantes de la revendication 1 sont connues de l'état de la technique pour protéger contre la copie de données numériques stockées sur un support d'informations:

   (1) une identification d'un chiffrage des données numériques (voir p. 1, l. 25-31);
   (2) une identification d'un tatouage des données numériques (voir p. 1, l. 32 - p. 2, l. 10).

   L'objet de la revendication 1 diffère de ces méthodes connues en ce que:

   (3) une identification d'un type non-enregistrable ou non-enregistrable du support d'informations;
   (4) une identification d'une signature cryptographique accompagnant les données numériques; et
   (5) une délivrance d'une permission ou d'une interdiction de copie et/ou de lecture desdites données numériques en fonction d'au moins deux éléments parmi (1)-(4).

   Le problème que se propose de résoudre la présente invention peut donc être considéré comme présentant une méthode améliorée pour protéger contre la copie de données numériques stockées sur un support d'informations.

Selon la description donnée dans les documents D1 et D2, les caractéristiques (3) et (4) présentent les mêmes avantages que ceux mentionnés dans la présente demande (voir D1, p. 8, l. 28 - p. 10, l. 36 en liaison avec fig. 4, particulièrement "step 50" et "step 54", et D2, abrégé, "Coupled with the combination of encrypting methods, an Authenticating Signature is recorded on the media only when copy-protection is required" et "when a copy of a protected CD is played, the absence of the Authenticating Signature causes the player to generate false data which prohibits the disk from playing normally"). Puisqu'on le sait généralement qu'en combinant des techniques indépendantes multiples l'exécution de la protection peut être améliorée (voir par exemple D3, abrégé), combiner l'ensemble des caractéristiques exposées dans la revendication 1 relève d'une démarche technique normale pour la personne du métier. L'objet de la revendication 1 n'implique par conséquent pas d'activité inventive (article 33(3) PCT).

3. Les caractéristiques ajoutées par les revendications 2-6 décrivent simplement des conditions alternatives pour permettre ou interdire de copie ou lecture les données numériques basées sur les méthodes (1)-(4). Par conséquent, l'objet des revendications 2-6 n'implique pas d'activité inventive non plus.

4. Les caractéristiques ajoutées par la revendication 7 (une conversion des données numériques en signaux analogiques et une altération des signaux analogiques si une interdiction de copie numérique est délivrée) sont implicitement révélées dans D1 aussi (voir p. 8, l. 1-27 et fig. 3). Par conséquent, l'objet de la revendication 7 n'implique pas d'activité inventive non plus. La même objection s'applique également pour la revendication 8.

5. La revendication 9 comporte seulement des caractéristiques d'un dispositif avec la fonction correspondant aux caractéristiques de méthode selon la revendication 1. En conséquence, l'objection faite en ce qui concerne la revendication 1 est également valide pour la revendication 9.

Concernant le point VII

Irrégularités dans la demande internationale

1. Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D1-D3 et ne cite pas ces documents.

2. La description ne cite pas de document reflétant l'état de la technique décrit à la pages 1-2 (règle 5.1 a) ii) PCT).

PROTECTION CONTRE LA COPIE DE DONNEES NUMERIQUES STOCKEES SUR UN SUPPORT D'INFORMATIONS

L'invention concerne une méthode et un dispositif permettant de protéger contre la copie de données numériques stockées sur un support d'informations.

Une possibilité inhérente aux données numériques est qu'elles peuvent être copiées sans perte notable de qualité puisque la copie consiste à transmettre de la source à l'enregistreur une série de « 1 » et de « 0 ». Le plus grand nombre d'erreurs survenant éventuellement lors de la copie peuvent être palliées en utilisant des méthodes de correction d'erreur. Ainsi lorsqu'un support d'informations contient des données numériques, il est en principe relativement simple d'enregistrer à l'identique sur un support enregistrable le contenu du support d'informations.

De nombreux types et sortes de supports d'informations sont utilisés pour stocker de l'information de toute nature sous forme numérique. Par exemple une bande magnétique, un disque optique enregistrable ou non (CD, CD-R, CD-RW, DVD, DVD-R, disque Magneto-optique etc., respectivements de l'anglais Compact Disc, CD-Recordable, CD-Read Write, Digital Versatile Disc, DVD-Recordable) peut stocker de l'information audio et / ou vidéo sous forme numérique.

Afin de mieux préserver par exemple les intérêts des auteurs de l'information stockée ou ceux de producteurs de support d'informations préenregistré, il est désirable de limiter les possibilités de copier librement et simplement les données numériques. Divers mécanismes et possibilités existent actuellement pour protéger des données numériques contre une copie illégitime.

De façon connue les données numériques peuvent être chiffrées lorsqu'elles sont stockées sur le support d'informations. Le chiffrage permet de limiter l'utilisation des données numériques au détenteur d'une clé publique ou privée de déchiffrage. Le chiffrage est par exemple utilisé dans la protection de données sur les DVD, disques optiques utilisés pour stocker des données vidéo sous forme numérique. Ainsi un lecteur de DVD nécessite une clé appropriée pour déchiffrer les données lues sur le DVD.

Une façon de protéger des données numériques contre la copie consiste à les doter d'un tatouage, c'est-à-dire de données auxiliaires attachées aux données numériques. Le tatouage doit être non-modifiable et non effaçable. La lecture des données se fait à l'aide d'une clé publique qui identifie le tatouage.

L'information de gestion des générations ne permet pas d'éviter en soi les copies par voie analogique.

Un objet de l'invention consiste à trouver une solution de protection contre la copie numérique dans laquelle aucune information relative à la génération de copie est disponible en clair lors de la copie.

Un autre objet de l'invention consiste à trouver une solution dans laquelle aucune modification de données relatives à la protection contre la copie soit entreprise à l'enregistrement éventuel d'une copie.

Une solution que propose l'invention prévoit une méthode de protection contre la copie de données numériques stockées sur un support d'informations, comprenant

une première identification d'un chiffrage des données numériques,

une seconde identification d'un tatouage de données numériques,

une première détermination d'une première marque si le chiffrage et le tatouage ont pu être identifiés,

une troisième identification d'un type du support d'informations,

une seconde détermination d'une seconde marque si la première marque a pu être déterminée et si un type déterminé de support d'informations a pu être identifié,

une quatrième identification de données de signature cryptographique accompagnant les données numériques,

une troisième détermination d'une troisième marque si la seconde marque a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée,

une première délivrance d'une permission de copie numérique des données numériques si la troisième marque a pu être déterminée.

Une première réalisation avantageuse de l'invention prévoit une seconde délivrance d'une interdiction de lecture des données numériques si la première identification est négative et si le tatouage a pu être identifié, ou si le chiffrage a pu être identifié et la seconde identification est négative.

Une deuxième réalisation avantageuse de l'invention prévoit une troisième délivrance d'une permission de copie numérique des données numériques si la première et la seconde identifications sont négatives.

Une troisième réalisation avantageuse de l'invention prévoit une quatrième délivrance d'une interdiction de copie numérique des données numériques si la première marque a pu être déterminée et si la troisième identification révèle un type différent du type déterminé de support d'informations.

Une quatrième réalisation avantageuse de l'invention prévoit une cinquième délivrance d'une interdiction de copie numérique des données numérique si la deuxième marque a pu être déterminée et si la quatrième identification est négative.

Une cinquième réalisation avantageuse de l'invention prévoit une conversion des données numériques en signaux analogiques et une altération des signaux analogiques si la première, la quatrième ou la cinquième délivrance a été réalisée.

Une sixième réalisation avantageuse de l'invention prévoit que l'interdiction de copie numérique comprend une suppression de sortie des données numériques.

-Une autre solution que propose l'invention prévoit un dispositif de lecture de données numériques stockées sur un support d'informations comprenant au moins,

une sortie numérique permettant de livrer des signaux représentatifs des données numériques lors d'une lecture des données numériques,

une sortie analogique permettant de livrer des signaux analogiques représentatifs des données numériques lors d'une lecture des données numériques,

un système de déchiffrage pour les données numériques permettant notamment d'établir si les données numériques sont chiffrées et si oui de déchiffrer les données numériques chiffrées, d'identifier si les données numériques comportent un tatouage et/ou des données de signature cryptographique, et d'identifier un type du support d'informations,

un système de protection pour la copie des données numériques recevant des signaux du système de déchiffrage pour les évaluer, et générant un signal de permission de copie dans le cas où les données numériques sont chiffrées, ont un tatouage, sont sur une support de type non-enregistrable et possèdent des données de signature cryptographique,

une partie de contrôle de l'enregistrement qui permet de gérer un flux de données numériques vers la sortie numérique lorsqu'elle reçoit notamment un signal de permission de copie,

un système de protection pour la lecture recevant des signaux du système de déchiffrage et générant un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées, ou lorsque les données numériques sont chiffrées mais non tatouées,

une partie de contrôle de la lecture qui permet d'interrompre la lecture des données ou leur sortie vers la sortie analogique lorsqu'elle reçoit notamment un signal d'interdiction de lecture.

Dans la suite, des exemples de réalisation sont présentés qui permettront d'illustrer et de mieux comprendre l'invention, en faisant référence aux figures 1 à 8, brièvement décrites ci-dessous :

Fig. 1 contient un organigramme illustrant un mode de réalisation de l'invention,

Fig. 2 à 5 contiennent des organigrammes illustrant des aspects de l'invention,

Fig. 6 contient un organigramme illustrant une conversion numérique-analogique selon l'invention,

Fig. 7 contient un schéma illustrant un dispositif selon l'invention.

La Fig. 1 contient un organigramme dans lequel des données numériques stockées sur un support d'informations 1 sont soumises à une première identification d'un chiffrage 2 afin de vérifier si les données numériques sont stockées sous forme chiffrée, puis à une seconde identification d'un tatouage 3 pour voir si les données sont pourvues d'un tatouage numérique. Une première bifurcation 4 permet de distinguer les cas où un chiffrage est identifié 5 ou non 6. Une seconde bifurcation 7 permet de distinguer les cas où un tatouage est identifié 8 ou non 9. Si les cas 5 et 8 sont vérifiés une première détermination 10 génère une première marque #1.

Une troisième identification 11 d'un type du support d'informations 1 sert à voir si le support d'informations est par exemple du type non-enregistrable ou enregistrable. Une information sur le type peut être contenue dans les données numériques en soi où résulter de mesures physiques de paramètres du support d'informations 1 lors par exemple d'une initialisation dans un lecteur du support d'informations 1. Une troisième bifurcation 12 permet de distinguer les cas où le

type serait d'un type déterminé 13, par exemple un support d'informations non enregistrable tel qu'un disque optique pressé, ou non 14. Si le cas 13 est vérifié et la première marque #1 a été générée alors une seconde détermination 15 génère une seconde marque #2.

Une quatrième identification 16 de données de signature cryptographique vérifie si les données numériques possèdent une signature cryptographique. Une quatrième bifurcation 17 permet de distinguer les cas où la signature cryptographique est présente 18 ou non 19. Si le cas 18 est vérifié et la seconde marque #2 a été générée alors une troisième détermination 20 génère une troisième marque #3.

En présence de la troisième marque #3 une première délivrance 21 d'une permission de copie numérique 22 des données numériques est réalisée.

Globalement l'organigramme de la Fig. 1 montre comment divers critères afférents aux données numériques mais aussi au support d'informations peuvent mener à la délivrance d'une permission de copie numérique, l'idée étant de ne permettre une copie que dans des conditions définies. Par exemple les données ne doivent pas avoir été manipulées donc doivent être chiffrées et tatouées. Ensuite les données ne doivent pas encore avoir été copiées. Si les données sont sur un disque non-enregistrable alors a priori les données sont sur un support d'informations d'origine. Finalement les données doivent posséder une signature cryptographique. Celle-ci indique que les données peuvent être copiées. C'est alors que les données reçoivent la permission de copie numérique. Un résultat de la copie des données sera identique à l'original sauf en ce qui concerne le support d'informations qui devra être enregistrable. Une nouvelle copie des données à partir du support d'informations enregistrable serait impossible car la deuxième marque #2 ne pourrait être générée après la troisième identification 11. En effet la troisième bifurcation 12 nous mènerait dans le cas 14.

D'autres cas de figure sont à envisager lorsque par exemple le chiffrage ou le tatouage des données numériques ne peuvent être identifiés. Normalement le chiffrage et le tatouage vont de pair et l'absence de l'un ou de l'autre est un indice de manipulation illicite des données numériques. Il s'agit alors d'aller plus loin que de simplement interdire la copie des données numériques. Il faut empêcher la lecture de celles-ci.

Un organigramme dans la Fig. 2 illustre deux cas de figure où le chiffrage et le tatouage ne sont pas identifiés ensembles. Un cas de figure prévoit que la première bifurcation 4 livre le cas 6, c'est-à dire que la première identification d'un chiffrage est négative, et que la seconde bifurcation 7 livre le

cas 8, c'est-à dire qu'un tatouage est présent. Alors une seconde délivrance 23 génère une interdiction de lecture des données numériques 24. En pratique cela pourrait par exemple conduire à une interruption de la lecture des données. Un autre cas de figure prévoit que la première bifurcation 4 livre le cas 5, c'est-à dire qu'un chiffrage est identifié, et que la seconde bifurcation 7 livre le cas 9, c'est -à dire que la seconde identification d'un tatouage est négative. Dans cet autre cas la seconde délivrance génère l'interdiction de lecture 24.

La méthode décrite permet de copier librement des données numériques qui ne sont pas protégées, par exemple des données dépourvues de chiffrage et de tatouage. La Fig. 3 contient un organigramme dans lequel la première et la seconde bifurcation 4 et 7 livrent chacune un cas d'identification négative respectivement les cas 6 pour le chiffrage et 9 pour le tatouage. Une troisième délivrance 25 génère alors directement la permission de copie numérique 22.

Dans le dernier cas il importe peu que les données soient sur un support d'informations enregistrable ou non. L'absence de chiffrage et de tatouage indique un niveau de protection des données minimum.

Dans certains cas de figure les données doivent pouvoir être lues et exploitées mais non copiées. C'est le cas notamment lorsque l'on achète un support d'informations contenant des données numériques dont l'auteur ou le producteur veut éviter la copie. C'est le cas également lorsqu'un support d'informations enregistrable contenant des données copiées légalement est lu. Un tel cas est illustré à l'aide d'un organigramme dans la Fig. 4 où une quatrième délivrance 26 vérifie que la première marque #1 a été délivrée et que le cas 14 d'identification d'un type de support d'informations différent du type déterminé a eu lieu avant de générer une interdiction de copie 27. En pratique le lecteur devrait mettre en oeuvre un dispositif empêchant une copie des données numériques, par exemple en inhibant une sortie numérique du lecteur.

Un autre tel cas est illustré à l'aide d'un organigramme dans la Fig. 5. Si la deuxième marque #2 est identifiée et le cas 19 signalise une quatrième identification négative, c'est à dire qu'aucune signature cryptographique permettant une copie des données est présente, alors une cinquième délivrance 28 génère l'interdiction de copie 27.

Il est entendu que le fait qu'aucune signature cryptographique permettant une copie des données ne soit identifiée n'exclut pas la présence d'une signature cryptographique particulière interdisant la copie.

Tout au long de la description il a déjà été fait mention du fait que le support d'informations 1 est utilisé dans un lecteur approprié. Les données numériques stockées sur le support d'informations 1 peuvent être dans certains cas acheminées vers une sortie numérique du lecteur. Dans l'exemple d'un lecteur DVD (disque optique pour données numériques vidéo/audio), une sortie numérique peut être prévue pour sortir un signal représentatif des données vers un lecteur / enregistreur DVD-R (ou autre) aux fins d'une copie, ou vers un ordinateur pour faire du traitement d'images. En général le lecteur prévoit aussi une sortie analogique afin de pouvoir transmettre un signal analogique représentatif des données numériques vers l'entrée analogique par exemple d'un téléviseur.

Un organigramme dans la Fig. 6 indique par une flèche pointillée que le support d'informations livre des données numériques 29. Une conversion 30 permet de convertir les données numériques 29 en signaux analogiques 31. Une présence de la permission de copie numérique 22 ensemble avec l'une quelconque des première, seconde ou troisième marques (#1, #2, #3), ou une présence de l'interdiction de copie numérique 27, est détectée dans une détection 32 qui le cas échéant déclenche une altération 33 des signaux analogiques pour obtenir des signaux analogiques altérés 34. Les signaux analogiques sont par exemple altérés de façon à ce qu'ils puissent être utilisés pour obtenir des images sur un téléviseur mais qu'il soit impossible de les copier à l'aide d'un magnétoscope à entrée analogique.

Avantageusement il est prévu une suppression à une sortie numérique du lecteur des données numériques 35 en présence de l'interdiction de copie numérique 27.

Le chiffrage des données numériques sur le support d'informations se fait normalement du coté du producteur.

Les données numériques ainsi que la signature cryptographique qui y est éventuellement associée sont déchiffrées dans le lecteur de données. Mais lorsque ces données doivent être transmises sur une sortie numérique du lecteur, les données sont chiffrées.

Un dispositif de lecture de données numériques 42 illustré à la Fig. 8 comprend une sortie numérique 43 qui permet de livrer des signaux représentatifs des données numériques lors d'un lecture des données numérique d'un support d'informations. Cette sortie 43 peut par exemple être réalisée à l'aide d'un bus numérique au standard IEEE1394. Une sortie analogique 44 permet de livrer des signaux analogiques représentatifs des mêmes données numériques. Un système de déchiffrage 45 permet de déchiffrer des données numériques si celles-ci sont

chiffrées, mais aussi d'identifier un éventuel tatouage et des données de signature cryptographique. Le système de déchiffrage permet de mettre en oeuvre par exemple les identifications 2, 3, 11 et 16 de la méthode illustrée à la Fig. 1.

Un système de protection contre la copie des données numériques 46 utilise des signaux émis par le système de déchiffrage 45 et les évalue en implémentant les déterminations 10, 15 et 20 de la méthode illustrée à la Fig. 1, et délivre après avoir déterminé les marques #1, #2 et #3 un signal de permission de copie.

Une partie de contrôle de l'enregistrement 47 permet de gérer un flux de données numériques vers la sortie numérique. Cette partie peut notamment activer le flux lorsqu'elle obtient du système de protection 46 le signal de permission de copie.

Le système de protection contre la copie des données numériques 46 peut également jouer le rôle d'un système de protection contre la lecture. Ce dernier système génère à l'aide des signaux reçus du système de déchiffrage 45 un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées ou encore lorsque les données numériques sont chiffrées mais non tatouées.

Une partie de contrôle de la lecture 48 permet d'interrompre la lecture des données numériques lorsqu'elle reçoit le signal d'interdiction du système de protection contre la lecture 46.

32. détection
33. altération
34. signaux analogiques altérés
35. suppression de sortie des données numériques
42. dispositif de lecture de données numériques
43. sortie numérique
44. sortie analogique
45. système de déchiffrage
46. système de protection pour la copie des données numériques
47. partie de contrôle de l'enregistrement
48. partie de contrôle de la lecture.

Revendications

1. Méthode de protection contre la copie de données numériques stockées sur un support d'information consistant à délivrer une permission ou une interdiction de copie *et/ou* de lecture desdites données numériques en fonction de l'identification ou non d'au moins deux éléments parmi :

- un chiffrage desdites données numériques ;
- un tatouage desdites données numériques ;
- un type enregistrable ou non-enregistrable dudit support d'information ;
- une signature cryptographique accompagnant lesdites données numériques.

2. Méthode selon la revendication 1, caractérisée en ce qu'une permission de copie numérique (22) est délivrée (21) lorsque :

- un chiffrage (2) desdites données numériques a été identifié ;
- un tatouage (3) desdites données numériques a été identifié ;
- un type de support (11) non-enregistrable a été identifié ; et
- une signature cryptographique (16) accompagnant lesdites données numériques a été identifiée.

3. Méthode selon la revendication 1, caractérisée en ce qu'une permission de copie numérique (22) est délivrée (25) lorsque :

- un chiffrage (2) desdites données numériques n'a pas été identifié ; et
- un tatouage (3) desdites données numériques n'a pas été identifié.

4. Méthode selon la revendication 1, caractérisée en ce qu'une interdiction de lecture (24) desdites données numériques est délivrée lorsque :

- un chiffrage (2) desdites données numériques n'a pas été identifié ; et
- un tatouage (3) desdites données numériques a été identifié.

5. Méthode selon la revendication 1, caractérisée en ce qu'une interdiction de copie (27) est délivrée (26) lorsque :

- un chiffrage (2) desdites données numériques a été identifié ;
- un tatouage (3) desdites données numériques a été identifié ; et
- un type de support (11) enregistrable a été identifié.

6. Méthode selon la revendication 1, caractérisée en ce qu'une interdiction de copie (27) est délivrée (28) lorsque :

- un chiffrage (2) desdites données numériques a été identifié ;
- un tatouage (3) desdites données numériques a été identifié ;
- un type de support (11) non-enregistrable a été identifié ; et
- aucune signature cryptographique (18) accompagnant lesdites données numériques n'a été identifiée.

7. Méthode selon l'une des revendications 1, 2, 5 ou 6, caractérisée en ce qu'elle comprend :

- une conversion (30) des données numériques (29) en signaux analogiques (31) ; et
- une altération (33) des signaux analogique si une interdiction de copie numérique (27) est délivrée.

8. Méthode de protection selon l'une quelconque des revendications 5 ou 6, caractérisée en ce que l'interdiction de copie numérique (27) comprend une suppression (35) de sortie des données numériques.

9. Dispositif de lecture de données numériques stockées sur un support d'informations comprenant au moins :

une sortie numérique (43) pour délivrer des signaux représentatifs des données numériques lors d'une lecture desdites données numériques ;

une sortie analogique (44) pour délivrer des signaux analogiques représentatifs des données numériques lors d'une lecture desdites données numériques ;

des moyens (45) de détection :

- d'un chiffrage desdites données numériques ;
- d'un tatouage desdites données numériques ;
- d'un type enregistrable ou non enregistrable dudit support d'information ;
- d'une signature cryptographique accompagnant lesdites données numériques ;

un système pour déchiffrer lesdites données numériques lorsqu'un chiffrage est détecté ;

un système de protection (46) contre la copie desdites données numériques recevant des signaux desdits moyens (45) de détection et générant

un signal de permission de copie (22) ou un signal d'interdiction de copie (27) en mettant en œuvre la méthode selon l'une des revendications 2 et 4 à 6 ;

des moyens de contrôle (47) de l'enregistrement supprimant les signaux délivrés à la sortie numérique (43) lorsque lesdits moyens de contrôle reçoivent un signal d'interdiction de copie (27) du système de protection (46) ;

un système de protection (46) de la lecture recevant des signaux desdits moyens (45) de détection et générant un signal d'interdiction de lecture (24) en mettant en œuvre la méthode selon la revendication 3 ; et

des moyens de contrôle de la lecture (48) interrompant la lecture des données ou leur sortie vers la sortie analogique (44) lorsque lesdits moyens de contrôle reçoivent un signal d'interdiction de lecture du système de protection (46).

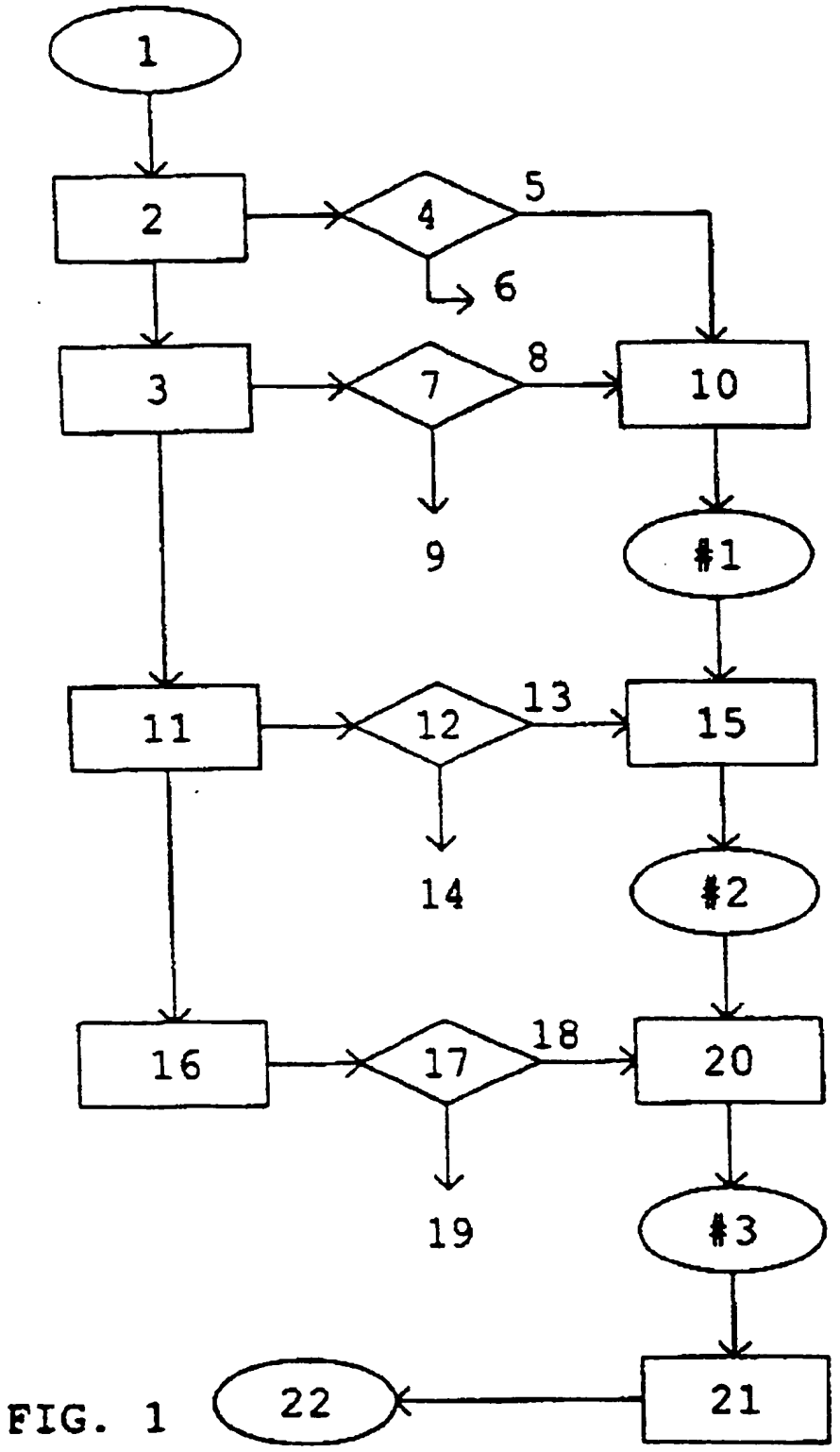


FIG. 1

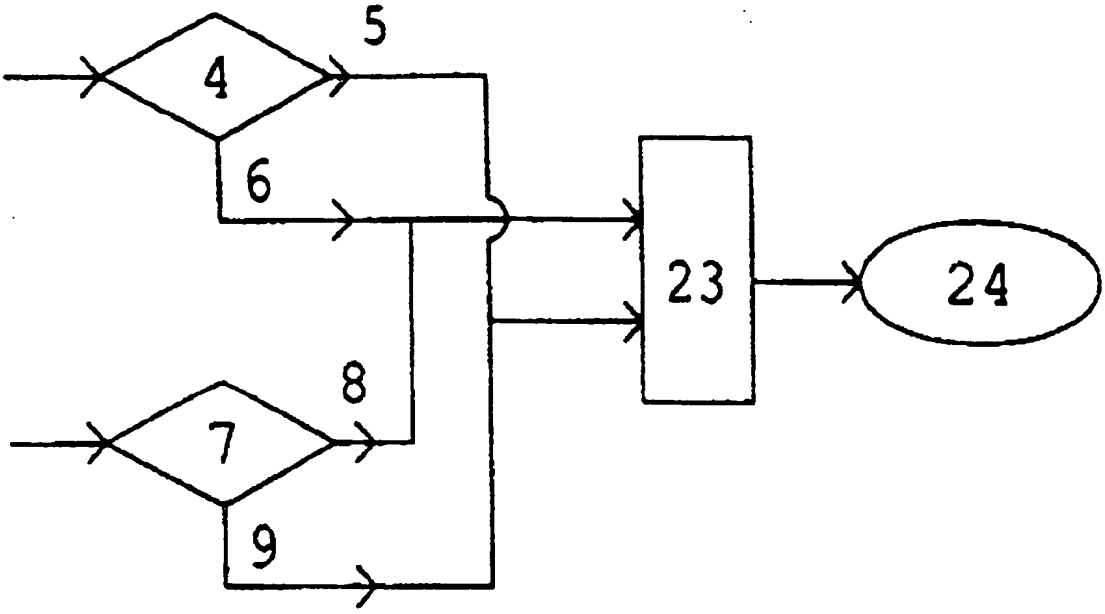


FIG. 2

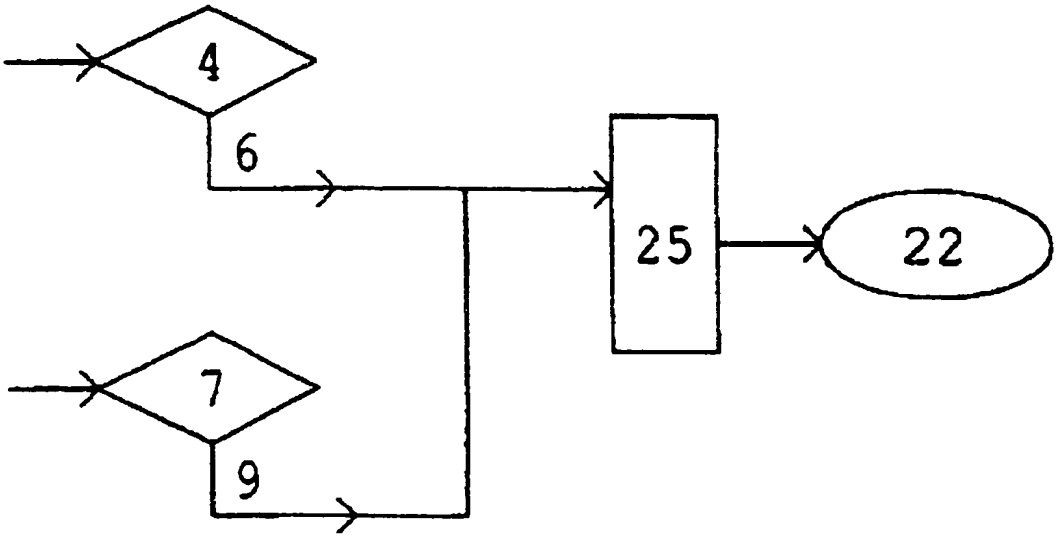


FIG. 3

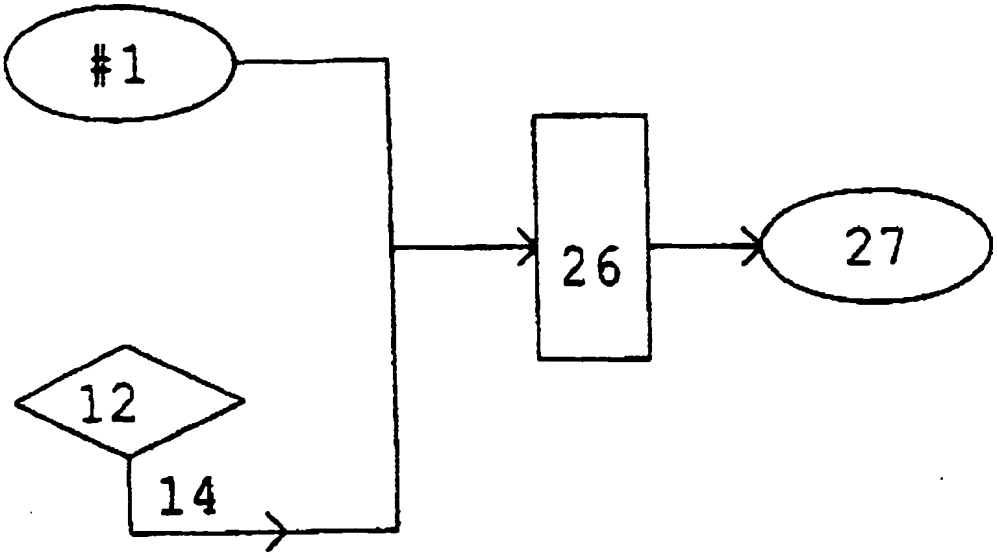


FIG. 4

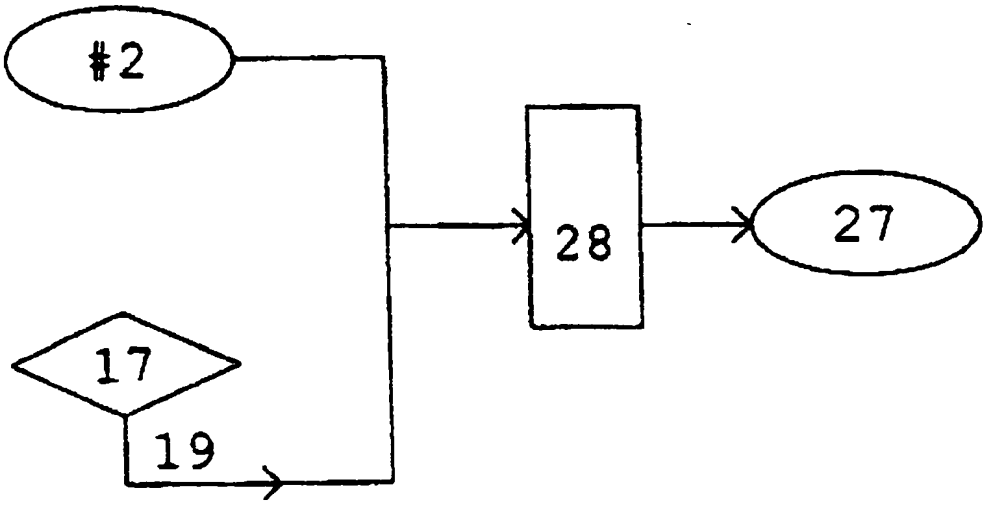


FIG. 5

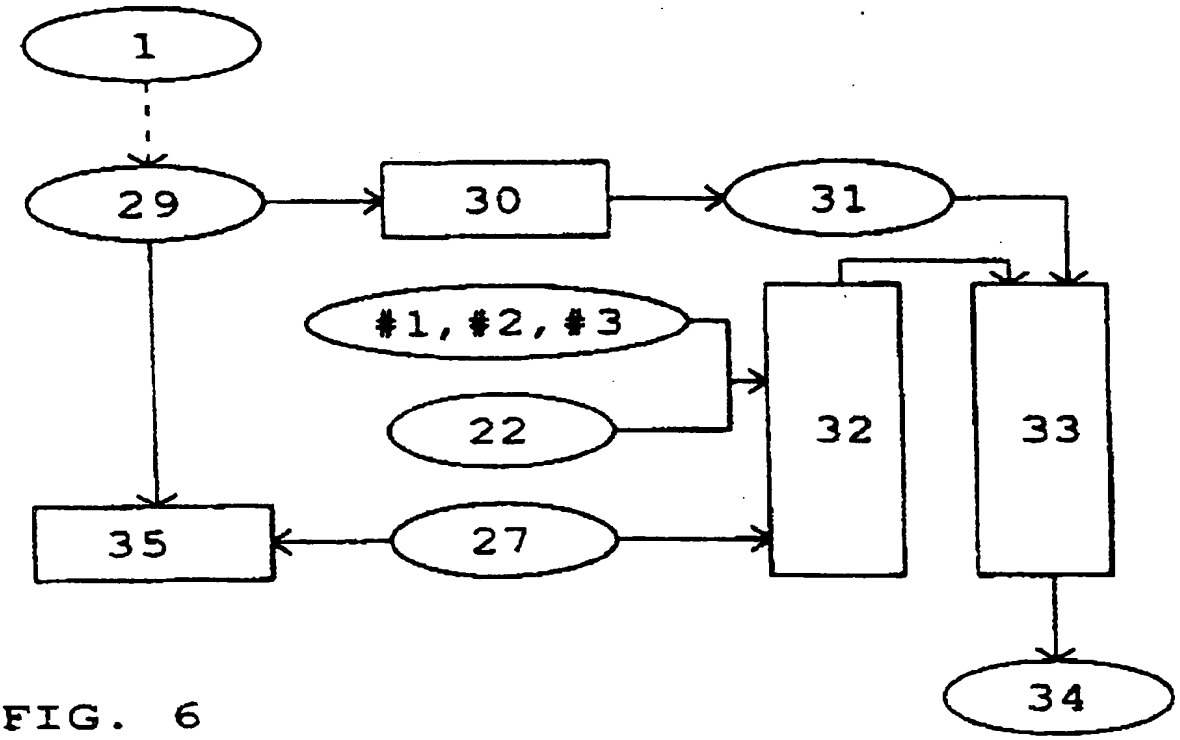


FIG. 6

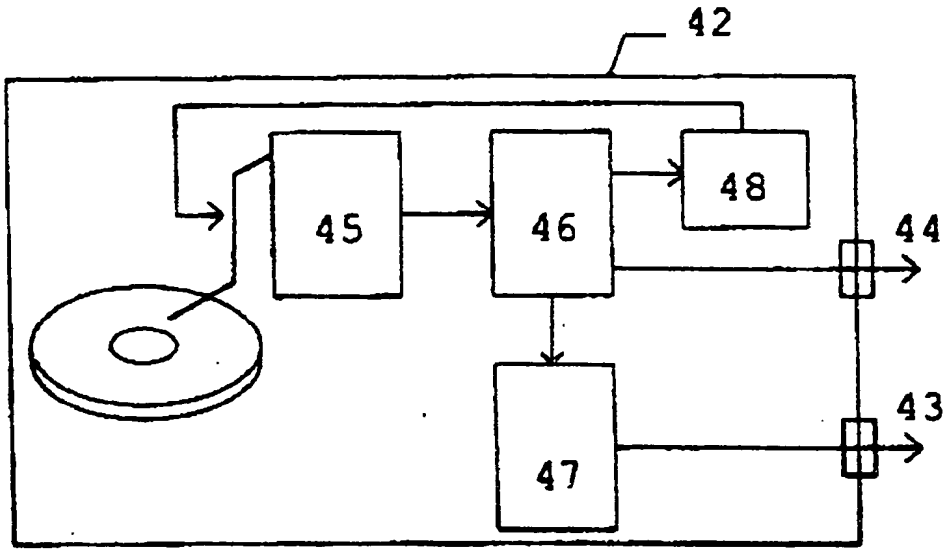


FIG. 7

09/787722

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PF980065	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/02267	International filing date (*day/month/year*) 23 September 1999 (23.09.99)	Priority date (*day/month/year*) 23 September 1998 (23.09.98)
International Patent Classification (IPC) or national classification and IPC G11B 20/00		
Applicant THOMSON MULTIMEDIA		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 16 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 11 April 2000 (11.04.00)	Date of completion of this report 08 November 2000 (08.11.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/02267

I. Basis of the report

1. With regard to the **elements** of the international application:*

RECEIVED
JUL 0 2 2001
Technology Center 2100

☐ the international application as originally filed

☒ the description:

pages 2, 10 , as originally filed

pages , filed with the demand

pages 1, 3-9, 11 , filed with the letter of 20 October 2000 (20.10.2000)

☒ the claims:

pages , as originally filed

pages , as amended (together with any statement under Article 19

pages , filed with the demand

pages 1-9 , filed with the letter of 20 October 2000 (20.10.2000)

☒ the drawings:

pages , as originally filed

pages , filed with the demand

pages 1/4-4/4 , filed with the letter of 20 October 2000 (20.10.2000)

☐ the sequence listing part of the description:

pages , as originally filed

pages , filed with the demand

pages , filed with the letter of

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-9	**YES**
	Claims		**NO**
Inventive step (IS)	Claims		**YES**
	Claims	1-9	**NO**
Industrial applicability (IA)	Claims	1-9	**YES**
	Claims		**NO**

2. Citations and explanations

1. The following documents are referred to:

D1: WO-A-9733283 (TIME WARNER ENTERTAINMENT CO) 1997-09-12;
D2: WO-A-9600963 (MACROVISION CORP) 1996-01-11;
D3: EP-A-0 413 350 (TOKYO SHIBAURA ELECTRIC CO) 1991-02-20.

Documents D1 and D2 are not cited in the international search report.

2. According to the description, the following features of Claim 1 are known from the prior art for copy protection of digital data stored on a medium:

(1) recognition of numerical data encryption (see p. 1, lines 25 to 31);

(2) recognition of tattooing on numerical data (see p. 1, lines 32 to p. 2, l. 10).

The subject matter of Claim 1 differs from those known methods as follows

(3) recognition of a recordable or of a non-recordable type of medium:

(4) recognition of a cryptographic signature with the digital data; and

(5) allowing or preventing copying and/or reading of said digital data on the basis of at least two of the elements (1) to (4).

The problem which the present application sets out to solve may thus be considered to be that of putting forward an improved method to protect against copying digital data stored on a medium.

According to the description given in documents D1 and D2, features (3) and 4) offer the same advantages as those mentioned in the present application (see D1, p. 8, l. 28 to p. 10, l. 36 together with Figure 4, especially "step 50"and "step 54", and the abstract of D2, "coupled with the combination of encrypting methods, an Authenticating Signature is recorded on the media only when copy-protection is required" and "when a copy of a protected CD is played, the absence of the Authenticating Signature causes the player to generate false data which prohibits the disk from playing normally"). As it is generally known that protection can be improved by combining several independent techniques (see, for example, the abstract of D3), to a person skilled in the art, combining the entirety of the features set out in Claim 1 would constitute a standard technical step. The subject matter of Claim 1 does not, therefore, involve an inventive step (PCT Article 33 (3)).

3. The features added by Claims 2 to 6 simply describe alternative ways, based on methods (1) to (4), of allowing or preventing digital data from being copied or read. Consequently, the subject matter of Claims 2 to 6 does not involve an inventive step either.

4. The features added by Claim 7 (converting digital data into analogue signals and deteriorating the analogue signals if digital copying is not authorised) are also implicitly revealed in D1 (see p. 8, l. 1 to 27 and figure 3). Therefore the subject matter of Claim 7 does not involve an inventive step either. The same objection also applies to Claim 8.

5. Claim 9 only comprises some features of a device whose function corresponds to the method features as per Claim 1. Consequently, the objection made relative to Claim 1 is also valid for Claim 9.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/02267

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1 (a) (ii), the description does not indicate the relevant prior art set out in documents D1 to D3, and does not cite those documents.

2. The description does not cite any document reflecting the prior art described on pages 1 and 2 (PCT Rule 5.1 (a) (ii)).